U.S. DoD

Remote Access

Protection Profile

for

High Assurance Environments

Version 1.0

June 2000

Document Authors:

G. Roger Black, National Security Agency (Team Leader)
John M. Boone, Mitretek Systems
Jerry Myers, The Aerospace Corporation
Edward A. Schneider, Institute for Defense Analyses

Acknowledgements:

The authors acknowledge the assistance of Lloyd E. Lutz, Jr. (Booz, Allen, and Hamilton), Faith Kramer (NSA), and Mark Mason (NSA). We wish also to acknowledge the hospitality of the Aerospace Corporation and Booz, Allen, and Hamilton for providing necessary resources and facilities during the development of the PP.

Table of Contents

Conventions and Terminology

Conventions

1 The notation, formatting, and conventions used in this Protection Profile are largely consistent with those used in version 2 of the Common Criteria (CC) [1]. Selected presentation choices are discussed here to aid the Protection Profile (PP) user.

2 The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this Protection Profile.

3 The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of functional requirements is denoted by bold text.

4 The selection operation is used to select one or more options provided by the CC in stating a requirement. The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Selections and assignments are both denoted by italicized text; however, one can determine which operation was performed by consulting the CC. From a specification viewpoint, only the words that result from the operation are important, not how the words were derived.

5 Whenever a selection or assignment operation is left incomplete in this PP, it is offset with brackets ("[]") and the text "ST selection" or "ST assignment," respectively, is indicated. These incomplete operations, along with their parameters, also appear in italicized text.

6 The iteration operation specifies use of a component more than a single time. There are several instances in this PP where components are iterated across partitions. Multiple use of components may occur when an operation within the component must be completed multiple times (with differing values), or for different allocation of functions to partitions of the TOE. Because all of the components in this PP are potentially iterated across partitions and each is allocated to a specific partition, every component has an identifier of the form $\text{COMPONENT}_{(\text{PARTITION}).}$ In this name, the main identifier (COMPONENT) refers to a standard CC identifier for a component, while the subscript (PARTITION) refers to the system partition to which the function is allocated.

7 It is possible that a component may be iterated within a partition. When this occurs, we add a semicolon (";") and a single, alphanumeric character as a suffix to the COMPONENT part of the identifier. Any alphanumeric character is valid, but typically the one chosen would have a mnemonic value. For example, for an identifier such as $\text{FCS\_COP.1;D}_{(\text{RU})}$, the ";D" suffix might stand for "data."

8 Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define “pass-fail” criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component.

Terminology

9 In the Common Criteria, many terms are defined in section 2.3 of Part 1. The following are a subset of those definitions. They are listed here to aid the user of the Protection Profile.

administrator — A defined role for the TOE, or any person that has assumed that role.

agent — An individual that is not an authorized user of the TOE.

authorized users — Any person that is authorized to access the TOE and who has successfully authenticated to the TOE.

COMM — Communications media partition.

CS — Communications server partition.

enclave — The secure facility that shelters and supports an IT environment on behalf of an organization.

ENV — The IT environment of the TOE.

partition — A division of the remote access system that defines the boundary for a unified set of logical and physical constraints.

remote users — An authorized user of the RU.

RU — Remote unit partition.

subject — On the CS, a subject is the set of processes associated with a role or a communication channel. On the RU, a subject is the set of all processes on the RU.

SYS — System partition.

unauthorized user — Any person that is not authorized, under the TOE’s security policies, to access the TOE.

10 This PP defines the following assets:

external communication channels — Communication links between the TOE and external IT systems.

internal communication channel — Communication links between the CS and the RU.

system resources — Any system assets (data and software) required for the correct operation of the TOE.

user resources — Any information assets (data and software) of authorized users.

Document Organization

Section 1 is the introductory material for the Protection Profile.

Section 2 provides a description of Remote Access Systems.

Section 3 is a discussion of the expected environment for a Remote Access System, in particular the assumptions that must be true about aspects such as physical, personnel, and connectivity conditions. This section then defines the set of threats that are to be addressed by either the technical countermeasures implemented in the Remote Access System's hardware and software, or through the environmental controls.

Section 4 defines the security objectives for both a Remote Access System and the environment in which it resides.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the Remote Access System.

Section 6 provides a rationale to explicitly demonstrate that the IT security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives; that each security objective is addressed by one or more relevant component requirements. Arguments are provided for the coverage of each objective. Next, Section 6 provides a set of arguments address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the PP requirements.

References are provided as background material for further investigation by interested users of the Protection Profile.

A list of acronyms is provided for frequently used terms.

1 INTRODUCTION

11 This Protection Profile (PP) was generated from a pilot program sponsored by the National Security Agency, Network Security Group, to develop a system-level protection profile. Remote Access, one of the sections of the Information Assurance Technical Framework (IATF), was selected as the system for the PP because it is believed to be a solution that will be used extensively throughout the DoD community.

12 This PP will be of use to a few audiences: Information System Security Engineers (ISSEs), product vendors, and system integrators. Members of the primary audience include ISSEs supporting the DoD community in designing secure information systems. The PP defines a minimal set of security requirements upon which a specific implementation of remote access can be built and against which the implementation can be tested. Secondarily, vendors may find this PP to be of value when they write product Security Targets (STs). Finally, system integrators may find this PP useful for identifying areas that need to be addressed to provide a secure system solution, but have not been explicitly dealt with by the products to be used.

13 Since writing this PP was part of a pilot program, the team also helped to refine the process of writing system-level PPs. The real usefulness of the PP can only be assessed after it is used for developing an actual secure remote access system. Feedback from such an effort should be incorporated into the PP and into the PP development process to ensure that future PPs provide value to future system engineering efforts.

14 Typically, system implementations are composed from a collection of components. A system integrator can then create a system-level Security Target from the STs for the individual components and show, based on compliance with the component STs and further testing, that the composition of components satisfy the system-level ST. Alternatively, component Protection Profiles can be written and the composition shown to satisfy the system-level PP.

15 The Remote Access protection profile team drew upon existing documentation that supports Remote Access solution design, the Network Security Framework Release 1.0 section 5.4 (Remote Access), and the existing solution developed by the Remote Access Security Program (RASP).

16 The team considered the RASP solution design as a worked example, but elevated the security requirements of that system in this PP in hopes of creating guidance that is reusable for design of future Remote Access system architectures. The architecture depicted in this PP closely resembles the IATF implementation guidelines for the Remote Access solution. Areas that deviate from this solution are documented in the appropriate sections.

17 Finally, the PP is written with future technology in mind. As it is impossible to predict future technological advances, an attempt was made to keep this document generic enough to incorporate new breakthroughs.

1.1 IDENTIFICATION

18 PP Identifier: U.S. DoD Remote Access Protection Profile for High Assurance Environments, Version 1.0. May 2000.

19 Criteria Version: This PP was developed using Version 2.1 of the Common Criteria (CC) [1].

20 Evaluation Assurance Level: EAL5.

21 Constraints: Targets of Evaluation (TOEs) developed to satisfy this Protection Profile shall conform to CC Part 2 and CC Part 3.

22 Registration: [TBD]

23 Keywords: Remote access, network security, remote unit, communications server.

1.2 PROTECTION PROFILE OVERVIEW

24 This Protection Profile specifies the DoD's minimum security need for remote access connection to a high-assurance enclave. The communications media for remote access may be outside the sphere of ownership and management of the enterprise making the remote connection. The requirements in this PP also contain several parameters that may be specified to fit the needs of a particular Remote Access system. Since this PP defines requirements for a system, the Target of Evaluation (TOE) may be composed from several inter-connected Security Targets. This PP specifies the security policies supported by the TOE and identifies the threats that are to be countered by the TOE. Furthermore, this PP defines implementation-independent security objectives of the system and its environment, defines the functional and assurance requirements, and provides the rationale for the security objectives and requirements. The environment, objectives, and requirements specified within this PP may not be applicable to all remote access scenarios.

1.3 RELATED PROTECTION PROFILES

25 U.S. DoD Remote Access Protection Profile for SBU-High Environments. [8]

26 U.S. DoD Communications Server Protection Profile. [9]

2 REMOTE ACCESS SYSTEM DESCRIPTION

27 A Remote Access System enables travelling or telecommuting users to securely access their local LANs, enclaves, or enterprise-computing environments via telephone or commercial data networks. The communication network is untrusted and may be shared with hostile users. The remote user's computing assets are physically vulnerable, especially when outside the United States, and must be protected. In particular, this equipment should be unclassified when it is either unattended or communicating with host terminals that are unauthorized to process equivalent sensitivity-level data.

28 In addition, the remote user should know when security features are enabled, and more importantly, when they are NOT! For example, because some features address secure communications, those features may not be enabled if the user is operating part of the system in a stand-alone mode. Also, the remote user will often not be operating in a physically protected environment. For that reason, the user should be able to secure the remote unit with a simple and effective emergency shutdown procedure.

29 This Protection Profile supports the scenario of remote access in a high-risk/high-assurance environment. Within this scenario, authorized users typically hold a clearance that makes them eligible to access classified information within the enclave, but may not have a need-to-know for all information within the enclave. Authorized users will connect to the enclave via a publicly owned communications media, such as a public switch telephone network or the Internet. Some requirements, such as those for assurance or cryptographic algorithms, may not be appropriate for information at some classification levels or for some other forms of networks than those described here.

30 The system has a natural decomposition into three logical components that reflect the fact that there are three distinctly different sub-environments that are part of the system environment: the environment local to a travelling user, the communications media environment, and the environment local to the enclave. The effectiveness of the security functional requirements at mitigating the risks from specific threats and the reliance upon non-IT security objectives have a similar decomposition associated with those three sub-environments. As a result, some of the functional security requirements of the TOE are only needed for a specific sub-environment.

31 For the convenience of specifying those requirements that need only apply to a portion of the TOE, there are three distinct TOE partitions that have been identified: a Remote Unit (RU) partition, a Communications Server (CS) partition, and a communications media partition (COMM). Because the COMM partition is typically owned and operated by private entities outside the control of the organization, this places a constraint on requirements levied on that partition. In this PP, no requirements are assigned to the COMM partition, although it is still useful to define this partition.

32 A RU partition contains those parts of the system that a user takes to a remote location, while the CS partition is the part of the system that remains within the security perimeter of the enclave and connects the enclave with the COMM partition. Requirements that are not a part of the TOE but on which the TOE may rely receive an environmental (ENV) designation, although the external environment is not considered a partition as such.

33 There may be many Remote Unit partitions in the system, while there is only one Communications Server partition.[1] The COMM, while part of the TOE, is outside the control of the organization operating the Remote Access System. Therefore, any security requirements applied to it are included with those for the system and ultimately must be satisfied by requirements on the RU and the CS.

34 Figure 2.1 illustrates the decomposition of the remote access system into its partitions. The security objectives and specific security functional requirements for this profile will each be identified as either applying to the entire system, the RU partitions, or the CS partition and they will be respectively marked with a subscript of SYS, RU, or CS. Similarly, some objectives and/or requirements will be marked with a subscript of ENV or COMM, where appropriate.

35

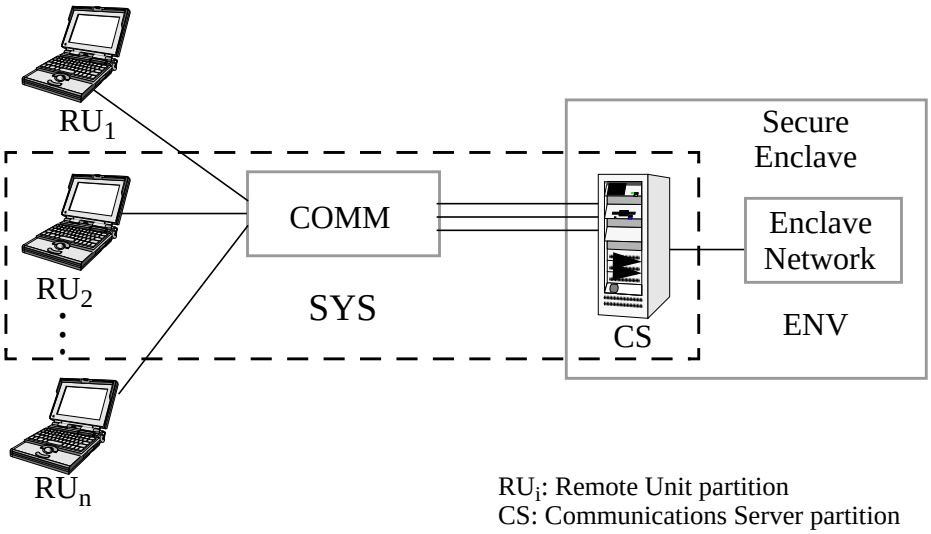

Figure 2.1 - Decomposition of the TOE

1. The use of multiple communications server devices to implement the Communications Server partition is not precluded by this restriction. The use of a single Remote Unit to communicate with two distinct Communications Server partitions in separate enclaves is not considered (nor is it precluded) by this profile.

36 Only the following interfaces exist to the system:

- the user interfaces to the RU (e.g. the keyboard, mouse, display, and hardware token interfaces);[2]
- the interface between the RU and the COMM;
- the interface between the COMM and the CS;
- the interface of the CS with the rest of the enclave; and,
- (possibly) a direct administrative console interface to the CS.

37 Any hardware or software required to encrypt/decrypt communications across the COMM is considered to be part of the RU or the CS.

38 Physical access from the environment (ENV) is significant but is not considered as an “interface” within this PP.

2. The term “hardware token” refers to a portable authentication device, which is only one example of an implementation that could be used to satisfy authentication security requirements on the RU.

3 SECURITY ENVIRONMENT

39 There are three distinct security environments that are relevant to this system: that of the CS, the COMM, and the RU. Because the TOE is intended to address a single "security problem," no distinction is made for these environments in the Policy and Threat statements, i.e., the reader can assume that all Policy and Threat statements apply to the "system" (SYS) partition. The generic security environment (ENV) is associated with the enclave with the understanding that the RU, being mobile, is sometimes located within that environment.

40 The CS environment is within a controlled facility and is closely analogous to a "traditional" IT security environment. It has an adequate administrative staff and is protected from physical access by unauthorized individuals.

41 The COMM is entirely outside the control of the organization, with the available controls being only what the COMM owner voluntarily provides. User access is not controllable and the environment is assumed to be hostile. Because the COMM is outside the scope of control for the organization, no security requirements can be attributed to it.

42 The RU environment is somewhere between the extremes of the CS and the COMM environments. Travelling users and telecommuters are both treated as "remote users" in this profile. Their environments apparently differ greatly in the degree of physical exposure to the remote computer when comparing, say, an international traveller to a local telecommuter. However, when taking into account the sensitivity of information to be protected by the TOE, the two environments can be characterized as roughly equal in terms of threat exposure.

3.1 ORGANIZATIONAL SECURITY POLICIES

43 The policies are derived from the following references:

a) EO 12958 (Sect 4.2), "Classified National Security Information" [4];[1]

b) DoDD-85xx.M&L (DRAFT), "Electronic Marking and Labeling" [5];[2]

c) OMB Cir. No. A-130, "Management of Federal Information Resources" [6]; and,

d) Memorandum from ASD(C3I), subject “Policy on Department of Defense (DoD) Electronic Notice and Consent Banner,” 16 January 1997 [7].

44 The TOE must provide uniform protection under the policies outlined here; hence, no distinction is made for the different TOE partitions with respect to organizational security policies. The determination of adequate policy coverage must take into account interpretations of subjective terms such as “eligible” and “adequate.” This interpretive aspect is addressed in the Rationale sections of the PP.

45 Table 3.1 lists the relevant organizational security policies.

Table 3.1 - Organizational Policies

Policy Name	Policy Statement
P.ACCOUNT	User activity shall be monitored to the extent that sanctions can be applied when malfeasance occurs, and to ensure that system controls are properly applied. All users will be notified that such monitoring may occur.
P.CONFIDENTIALITY	The confidentiality of user data must be protected.
P.ELGIBLE	Authorized users and administrators of the TOE shall be eligible to access information that is collected, created, communicated, computed, disseminated, processed, or stored on the TOE.
P.EXPORT	Authorized users and administrators of the TOE shall not export information processed by the TOE without proper and explicit authorization.
P.INTEGRITY	The integrity of user data must be protected.
P.MANAGE	The TOE shall be managed such that its security functions are implemented and preserved throughout its operational lifetime.
P.MARKING	User data must be adequately marked to describe the sensitivity of the information.

1. Some policy statements from this EO are transcribed as Assumptions.
2. This document has a basis in EO 12958.

3.2 THREATS TO SECURITY

46 The TOE must provide uniform protection against the threats outlined here; hence, no distinction is made for the different TOE partitions with respect to threats. The Rationale sections address the determination of adequate threat mitigation.

47 The attacks outlined in the specified threats may be motivated by deliberate malice or could be the result of unintentional mistakes on behalf of the improperly trained user. Results of a deliberate attack can be especially damaging to the organization's information system due to the attacker's advantage of knowing the network's configuration and thus its vulnerabilities.

48 Table 3.2 lists those Threats that are addressed by a remote access system that is compliant with this Protection Profile. All the malicious threat agents are considered to have high levels of expertise, resources, and motivation. "Malicious threat agents" are all unauthorized users and all authorized users or administrators violating their trust. The term "compromise" (when unqualified) refers to a degradation of the confidentiality and/or integrity of some asset.

Table 3.2 - Security Threats

Threat Name	Threat Statement
T.ALTER	An unauthorized user may surreptitiously gain access to the TOE and attempt to alter and/or replace system elements (e.g., hardware, firmware, or software) in an attempt to subvert the device.
T.CAPTURE	An unauthorized agent may eavesdrop on, or otherwise capture, data being transferred on a communications channel.
T.CRASH	The TOE may take actions based on security-critical data that, due to interruption of the operation of the TOE, is either incomplete or corrupted.
T.ERROR	An authorized user may attempt to perform unauthorized or erroneous actions that will compromise user and/or system resources.
T.IMPORT	An authorized user or administrator of the TOE may unwittingly introduce malicious code into the system, resulting in a compromise of the integrity and/or availability of user and/or system resources.
T.INTRUDE	An unauthorized user may use the TOE to gain access to the secure enclave.
T.MASQUERADE	An unauthorized user may attempt to gain access to the TOE by pretending to be an authorized user.
T.PHYSICAL	Security-critical parts of the TOE may be subject to physical attack by unauthorized agents, which may compromise security.
T.TRAFFIC	Use of the TOE may transmit (via traffic analysis or covert channel analysis) sensitive information to unauthorized users.

3.3 SECURE USAGE ASSUMPTIONS

49 Table 3.3 lists the relevant secure usage assumptions. The acronyms "CS," "RU," "SYS," and "COMM" refer to the TOE partitions and are used as suffixes to indicate the scope of the assumption.

Table 3.3 - Secure Usage Assumptions

Assumption Name	Assumption Statement
$A.CONTROLLED_{(RU)}$	Configuration and adminstistration of the RU are duties performed by TOE administrators.
$A.DEDICATED_{(CS)}$	The CS is a dedicated communications server and does not support general-purpose accounts or applications for individuals other than the designated administrators of the CS.
$A.FACILITY_{(CS)}$	The CS operates within a protected facility that provides protection against unauthorized physical access.
$A.TRUSTED\_ADMIN_{(SYS)}$	Administrators will not deliberately abuse their privileges so as to violate organizational security policies and are competent to manage the TOE and the information it contains.
$A.TRUSTED\_USER_{(SYS)}$	Authorized users of the RU will not intentionally violate organizational security policies and will exercise due care in the operation and use of the RU.

4 SECURITY OBJECTIVES

50 This section provides the TOE and environmental objectives in separate subsections.

4.1 SECURITY OBJECTIVES FOR THE TOE

51 Table 4.1 lists the IT security objectives for the TOE. The acronyms "CS," "RU," and "SYS" refer to TOE partitions and are used as suffixes to indicate the scope of the objective.

Table 4.1 - Security Objectives for the TOE

Objective Name	Objective Statement
O.ACCESS$_{(SYS)}$	The TOE will control access to information that is subject to the enclave security policy, based on the identity of the accountable individuals, such that this policy cannot be bypassed in the TOE.
O.AUDIT$_{(SYS)}$	The TOE will provide support for an audit trail to ensure each authenticated user and TOE administrator can be held accountable for his or her actions in the TOE. The audit trail will be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.
O.BANNER$_{(SYS)}$	The TOE will provide a banner to notify all users that they are entering a government computer system.
O.DETECT$_{(RU)}$	The RU will detect unauthorized changes to its configuration.
O.IDENTIFY$_{(SYS)}$	The TOE will uniquely identify and authenticate individuals.
O.MANAGE$_{(SYS)}$	The TOE will provide adequate management features for its security functions.
O.MEDIA$_{(RU)}$	The RU will protect sensitive data stored on it such that this data is unavailable while the TOE is not operating.
O.NO_EAVESDROP$_{(SYS)}$	The TOE will prevent, with a strength appropriate for tunneling classified data across a public network, the disclosure of information during transfers between a RU and the CS.
O.RECEIVE$_{(SYS)}$	A CS or a RU will only accept remote commands and data from another CS or RU with which it is mutually authenticated.
O.SELF-PROTECT$_{(SYS)}$	The TOE will protect its security-related functions against external interference or tampering by users, or attempts by users to bypass its security functions.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

52 Table 4.2 lists the IT security objectives for the environment. The acronyms "CS," "RU," "SYS," and "COMM" refer to the TOE partitions and are used as suffixes to

indicate the scope of the objective. These objectives will be satisfied largely through the application of procedural and/or administrative measures, although some will refer to technological components. The security objectives for the environment are presented separately for the CS, RU, and SYS partitions.

Table 4.2 - Security Objectives for the Environment

Objective Name	Objective Statement
OE.ACCREDITED$_{(SYS)}$	The enclave will be accredited to operate the TOE.
OE.ADMIN$_{(SYS)}$	Administrators manage the remote access system in a manner that maintains the system security.
OE.AUDIT$_{(CS)}$	Enclave personnel will apply technical, procedural, and administrative controls that are sufficient to maintain user accountability throughout the enclave.
OE.CLEARED$_{(SYS)}$	Authorized users and administrators must receive formal clearance before they can access the TOE.
OE.CRYPTOKEYS$_{(SYS)}$	The Department of Defense, Public Key Infrastructure will provide the necessary key initialization to support the CS/RU authentication function and the media encryption function on the RU.
OE.INSTALL$_{(SYS)}$	The remote access system is delivered and installed in a manner that maintains the system security.
OE.OPERATE$_{(RU)}$	Authorized users operate the RU in a manner that maintains the system security.
OE.PHYSICAL$_{(SYS)}$	TOE hardware, software, and documentation, and all classified data handled by the TOE are physically protected to prevent unauthorized (intentional or unintentional) disclosure.
OE.TRAINED$_{(SYS)}$	Train authorized users and administrators about relevant security policies and the practices they need to follow to establish and maintain adequate security.

5 SECURITY REQUIREMENTS

53 This section provides functional and assurance requirements that must be satisfied by a Protection Profile-compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1 SECURITY FUNCTIONAL REQUIREMENTS

54 This section provides information related to the TOE's Security Functional Requirements (SFRs). The first subsection addresses strength-of-function claims. The second subsection identifies standards compliance methods for the cryptographic SFRs included in this PP. The third subsection identifies the Security Function Policies (SFPs) used by the SFRs. The fourth subsection specifies the SFRs and related Application Notes.

5.1.1 STRENGTH OF FUNCTION CLAIMS

55 Security functions that implemented as probabilistic or permutational functions, except for cryptographic functions, shall have a strength-of-function (SoF) rating of SoF-High.

5.1.2 IDENTIFICATION OF STANDARDS COMPLIANCE METHODS

56 For this PP, cryptographic operations and key management functions must meet Type I specifications, including the use of Type-1 standard protocols. The methodology used to determine compliance to Type I standards will be specified by the Designated Approval Authority of the TOE-user organization. No additional compliance methods are required for this PP beyond those that already exist for Type I specifications.

5.1.3 IDENTIFICATION OF SFPS

57 The following SFP definitions are used within the functional requirements of this PP.

P.SEPARATE: User data may only flow within the CS between an RU connection and the associated enclave session.

P.RECEIVE:[1] An RU will only accept remote information from a CS with which it is registered, and the CS will only accept remote information from a registered RU.

58 Table 5.1 shows the use of these SFPs within components of this PP.

Table 5.1 - Components use of SFPs

Component	P.SEPARATE	P.RECEIVE
$FDP\_IFC.1_{(CS)}$	X	
$FDP\_IFF.1_{(CS)}$	X	
$FDP\_IFC.1_{(SYS)}$		X
$FDP\_IFF.1_{(SYS)}$		X
$FDP\_ITT.2_{(SYS)}$		X
$FDP\_ITT.3_{(SYS)}$		X
$FMT\_MSA.1_{(SYS)}$	X	X
$FMT\_MSA.3_{(SYS)}$	X	X

1. Note that P.RECEIVE does not exclude the possibility that a given RU may be registered with more than one CS.

5.1.4 FUNCTIONAL REQUIREMENTS

59 The functional security requirements for this Protection Profile consist of components from Part 2 of the CC, which are summarized in Table 5.2. Following the table, each component is listed individually, with Application Notes.

60 The iterations for cryptographic-related functions (FCS_COP and FCS_CKM) use a suffix to associate related functions and dependencies. The high degree of iteration for the FCS_COP functions is required to maintain independence of their key management dependencies. The “A” suffix stands for “authentication” encryption and shows the correct pairing for device authentication between the RU and CS. The “C” suffix stands for “communications” encryption and shows the correct pairing with RU and CS counterpart functions for encryption of communication data. Note that the TOE key management functions are associated with the communications encryption function. The “D” suffix stands for “disk” encryption and is used to distinguish the media encryption functions on the RU. This function is not paired with a CS counterpart.

Table 5.2 - - Functional Requirements

Functional Class	Component		Partition		
			CS	RU	SYS
Security Audit	FAU_ARP.1	Security alarms		X	
	FAU_GEN.1	Audit data generation	X		
	FAU_GEN.2	User identity association	X		
	FAU_SAA.3	Simple attack heuristics		X	
	FAU_STG.1	Protected audit trail storage	X		
	FAU_STG.4	Prevention of audit data loss	X		
Cryptographic Support	FCS_CKM.1;C	Cryptographic Key Generation			X
	FCS_CKM.2;C	Cryptographic Key Distribution			X
	FCS_CKM.4;C	Cryptographic Key Destruction			X
	FCS_COP.1;A	Cryptographic Operation (authentication)	X	X	
	FCS_COP.1;C	Cryptographic Operation (communications)	X	X	
	FCS_COP.1;D	Cryptographic Operation (disk)		X	
User Data Protection	FDP_IFC.1	Subset information flow control	X		X
	FDP_IFF.1	Simple security attributes	X		X
	FDP_ITT.2	Transmission separation by attribute			X
	FDP_ITT.3	Integrity monitoring			X
	FDP_RIP.2	Full residual information protection			X

Table 5.2 - - Functional Requirements

Functional Class	Component		Partition		
			CS	RU	SYS
Identification and Authentication	FIA_AFL.1	Authentication failure handling	X	X	
	FIA_ATD.1	User attribute definition			X
	FIA_UAU.2	User authentication before any action			X
	FIA_UAU.3	Unforgeable authentication			X
	FIA_UAU.6	Re-authenticating		X	
	FIA_UAU.7	Protected authentication feedback			X
	FIA_UID.2	User identification before any action			X
	FIA_USB.1	User-subject Binding	X		
Security Management	FMT_MOF.1	Management of security functions behaviour			X
	FMT_MSA.1	Management of security attributes			X
	FMT_MSA.2	Secure security attributes			X
	FMT_MSA.3	Static attribute initialisation			X
	FMT_MTD.1	Management of TSF data			X
	FMT_REV.1	Revocation			X
	FMT_SAE.1	Time-limited authorization	X		
	FMT_SMR.1	Security roles			X
Protection of the TOE Security Functions	FPT_FLS.1	Failure with preservation of secure state	X	X	
	FPT_ITT.2	TSF data transfer separation			X
	FPT_ITT.3	TSF data integrity monitoring			X
	FPT_RPL.1	Replay detection			X
	FPT_RVM.1	Non-bypassability of the TSP			X
	FPT_SEP.1	TSF domain separation			X
	FPT_STM.1	Reliable time stamps	X		
TOE Access	FTA_SSL.1	TSF-initiated session locking		X	
	FTA_TAB.1	Default TOE access banners			X

FAU_ARP.1$_{(RU)}$ Security alarms

FAU_ARP.1.1 The TSF shall take an alarm action to alert an authorized user of the RU upon detection of a potential security violation.

Note: This requirement applies specifically to unauthorized modifications of configuration data (e.g., BIOS data), for the period of time that the RU is in the field. For the RU in a remote access application, this function might best be implemented during start-up. This can be thought of as a "transitory function" in that it occurs at a specific point in time and does not perpetually exist while the TOE is in its operational state. Only minimal audit data (that necessary to trip the alarm) is required, and so this function does not depend upon FAU_GEN.1. Rather, this minimal audit data is accommodated by the "signature events" specified in FAU_SAA.3$_{(RU)}$. This function should apply only to configuration data that is relevant to the TOE.

FAU_GEN.1$_{(CS)}$ Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the minimum level of audit; and
c) The events listed in Table FAU_GEN.1.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, a session identifier and [ST assignment: other audit relevant information].

Note: Some events specified are at a CC audit level greater than minimum. For these events "minimum" is interpreted as "at least minimum."

FAU_GEN.1 does not list auditable event requirements for functional components associated with the RU partition (see Table FAU_GEN.1.1). The RU partition does not include an audit generation capability and so those functional components cannot generate audit records. Similarly, those auditable event requirements that apply to the SYS partition should be interpreted as applying only to the CS partition. There are no audit-related objectives associated with the RU partition.

FAU_GEN.1.1 lists specific audit requirements associated with functional components included in the profile, excluding the RU-specific functional

components. FAU_GEN.1.2, without modification, specifies most of the audit data required to address accountability concerns. The success or failure of events may sometimes be an implicit property of an audit record. This element adds “session identifier” to complement the intrinsically defined audit data requirements. Furthermore, this is an extensible element and allows the ST author to provide additional audit data detail.

Table FAU_GEN.1- Auditable Events

Component	Auditable Events
FAU_STG.4$_{(CS)}$	Actions taken due to the audit storage failure.
FCS_CKM.1;C$_{(SYS)}$ FCS_CKM.2;C$_{(SYS)}$ FCS_CKM.4;C$_{(SYS)}$	Success and failure of the activity.
FCS_COP.1;C$_{(CS)}$	Success and failure, and the type of cryptographic operation.
FDP_IFF.1$_{(CS)}$ FDP_IFF.1$_{(SYS)}$	Decisions to permit requested information flows. All decisions on requests for information flow.
FDP_ITT.2$_{(SYS)}$	Errors that occur in the transfer of user data.
FDP_ITT.3$_{(SYS)}$	Successful transfers of user data, including identification of the integrity protection method used.
FIA_AFL.1$_{(CS)}$	The reaching of the threshold for the unsuccessful authentication attempts. Actions (e.g. disabling of a terminal) taken upon reaching the threshold. Restoration to the normal state (e.g. re-enabling of a terminal).
FIA_UAU.2$_{(SYS)}$	All use of the authentication mechanism.
FIA_UAU.3$_{(SYS)}$	Detection of fraudulent authentication data.
FIA_UID.2$_{(SYS)}$	All use of the user identification mechanism, including the user identity provided.
FIA_USB.1$_{(CS)}$	Success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject).
FMT_MSA.2$_{(SYS)}$	All offered and rejected values for a security attribute.
FMT_REV.1$_{(SYS)}$	Unsuccessful revocation of security attributes.
FMT_SMR.1$_{(SYS)}$	Modifications to the group of users that are part of a role.
FPT_ITT.3$_{(SYS)}$	The detection of modification of TSF data.
FPT_RPL.1$_{(SYS)}$	Detected replay attacks.
FPT_STM.1$_{(CS)}$	Changes to the time.

FAU_GEN.2$_{(CS)}$ User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Note: Before remote users are authenticated, there may be audit data generated that is security relevant. For instance, the CS may record a lot of audit data associated with an intrusion attempt without ever being able to identify a valid user. In these cases a pseudo identity is acceptable, as long as activities can be associated with unique entities (e.g., via sessions). It should be possible to associate these activities with a specific user if that user successfully completes I&A.

FAU_SAA.3$_{(RU)}$ Simple attack heuristics

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events – unauthorized modifications to RU configuration data – that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of configuration data hashes.

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Note: Signature events are modifications to the RU BIOS or other configuration data by unauthorized users. The internal representation that is maintained by the TSF need not be generated at the same time the signature event occurs. However, the internal representation must be generated before the configuration data is used again. For instance, the TSF can apply the hash function that checks for modifications to configuration data at boot time.

FAU_STG.1$_{(CS)}$ Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records.

Note: Detection of modifications

FAU_STG.4$_{(CS)}$ Prevention of audit data loss

FAU_STG.4.1 The TSF shall [ST selection: ‘prevent auditable events,’ ‘overwrite the oldest stored audit records’] and [ST assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

Note: It is important that if overwriting the audit trail is implemented for the TOE, the period between audit trail overwrites be long enough to allow for necessary audit review tasks and/or off-loading of audit data (if desired). These considerations must also take into account that an attacker may purposely act with the intention of causing overwrites of the audit trail.

FCS_CKM.1;C$_{(SYS)}$ Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic session keys in accordance with a specified cryptographic key generation algorithm [ST assignment: Type 1 cryptographic key generation algorithm] and specified cryptographic key sizes [ST assignment: Type 1 cryptographic key sizes] that meet the following: [ST assignment: Type 1 cryptographic standards].

Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of classified information.

The cryptographic key generation system used in the current RAS configuration are Type II cryptographic algorithms with an 80 bit key length. Ideally Type I cryptographic algorithms with a minimum of a 128 bit key length are expected to be used for the protection of secret information. The user, in accordance with national security guidelines, should determine the appropriate algorithm to be used to protect their secret information.

FCS_CKM.2;C$_{(SYS)}$ Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic session keys in accordance with a specified cryptographic key distribution method [ST assignment: Type I cryptographic key distribution method].

Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of classified information.

FCS_CKM.4;$C_{(SYS)}$ Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic session keys in accordance with a specified cryptographic key destruction methods [ST assignment: Type I cryptographic key destruction method] that meets the following: [ST assignment: Type I list of standards].

Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of classified information.

FCS_COP.1;$A_{(CS)}$ Cryptographic Operation (CS authentication)

FCS_COP.1.1 The TSF shall perform CS to RU authentication in accordance with a specified cryptographic algorithm [ST assignment: Type I cryptographic algorithm] and cryptographic key sizes [ST assignment: Type I cryptographic key sizes] that meet the following: [ST assignment: Type I list of standards].

Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of classified information.

FCS_COP.1;$A_{(RU)}$ Cryptographic Operation (RU authentication)

FCS_COP.1.1 The TSF shall perform RU to CS authentication in accordance with a specified cryptographic algorithm [ST assignment: Type I cryptographic algorithm] and cryptographic key sizes [ST assignment: Type I cryptographic key sizes] that meet the following: [ST assignment: Type I list of standards].

Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of classified information.

FCS_COP.1;$C_{(CS)}$ Cryptographic Operation (CS communications)

FCS_COP.1.1 The TSF shall perform encryption of user data during transmission to the RU in accordance with a specified cryptographic algorithm [ST assignment: Type I cryptographic algorithm] and cryptographic key sizes [ST assignment: Type I cryptographic key sizes] that meet the following: [ST assignment: Type I list of standards].

Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of classified information.

FCS_COP.1;$C_{(RU)}$ Cryptographic Operation (RU communications)

FCS_COP.1.1 The TSF shall perform encryption of user data during transmission to the CS in accordance with a specified cryptographic algorithm [ST assignment: Type I cryptographic algorithm] and cryptographic key sizes [ST assignment: Type I cryptographic key sizes] that meet the following: [ST assignment: Type I list of standards].

Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of classified information.

FCS_COP.1;$D_{(RU)}$ Cryptographic Operation (RU disk)

FCS_COP.1.1 The TSF shall perform

a. cryptographic checksum on RU configuration data, and
b. encryption of application and user data on the RU,

in accordance with a specified cryptographic algorithm [ST assignment: Type I cryptographic algorithm] and cryptographic key sizes [ST assignment: Type I cryptographic key sizes] that meet the following: [ST assignment: Type I list of standards].

Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of classified information.

FDP_IFC.$1_{(CS)}$ Subset information flow control.

FDP_IFC.1.1 The TSF shall enforce the P.SEPARATE policy on user data.

Note: Information authorized by the enclave to be sent to a remote user should not be sent to another remote user, who may not be authorized to receive that information.

FDP_IFC.$1_{(SYS)}$ Subset information flow control.

FDP_IFC.1.1 The TSF shall enforce the P.RECEIVE policy on all COMM communications.

FDP_IFF.1$_{(CS)}$ Simple security attributes.

FDP_IFF.1.1 The TSF shall enforce the P.SEPARATE policy based on the following types of subject and information security attributes: remote user identity and enclave session identity.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: the remote user identity or the enclave session identity of the subject match that of user data that it accesses.

FDP_IFF.1.3 The TSF shall enforce: the remote user identity of a subject corresponds to the user identity of the enclave session identified by the subject's enclave session identity attribute.

FDP_IFF.1.4 The TSF shall provide the following: none.

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: none.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: none.

Note: The only requirement is to control information flow in the CS based on remote user and session identities. FDP_IFF.1.{4,5,6} add no additional requirements.

FDP_IFF.1$_{(SYS)}$ Simple security attributes.

FDP_IFF.1.1 The TSF shall enforce the P.RECEIVE policy based on the following types of subject and information security attributes: remote user identity.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: the remote user identity is registered with the CS.

FDP_IFF.1.3 The TSF shall enforce: none.

FDP_IFF.1.4 The TSF shall provide the following: none.

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: none.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: none.

Note: FDP_IFF.1.{3,4,5,6} add no additional requirements.

FDP_ITT.2$_{(SYS)}$ Transmission separation by attribute.

FDP_ITT.2.1. The TSF shall enforce the P.RECEIVE policy to prevent the disclosure or modification of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.2.2. The TSF shall separate data controlled by the SFP(s) when transmitted between physically-separated parts of the TOE, based on the values of the following: remote user identity.

Note: This is translated into FDP_UCT.1 for the RU and the CS when the TOE is decomposed. It relies on FCS_COP.1;C components.

FDP_ITT.3$_{(SYS)}$ Integrity monitoring

FDP_ITT.3.1 The TSF shall enforce the P.RECEIVE policy to monitor user data transmitted between physically-separated parts of the TOE for the following errors: modification of data, substitution of data, replay of data, and deletion of data.

FDP_ITT.3.2 Upon detection of a data integrity error, the TSF shall discard the affected data.

Note: This is translated into FDP_UIT.1 for the RU and the CS when the TOE is decomposed. It relies on FCS_COP.1;C components.

FDP_RIP.2$_{(SYS)}$ Full residual information protection.

FDP_RIP.2.1. The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from all objects.

Note: The resources include memory and communication channels when deallocated from classified processing. Typically communications-related objects include buffers and packets. Other objects that require protection include registers, memory, and file system objects.

FIA_AFL.1$_{(CS)}$ Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when an administrator-configurable number unsuccessful authentication attempts occur related to cumulative authentication failures of a specific user identity to a CS.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall lock the user out from future successful authentication to the CS.

Note: FIA_AFL.1.1 refers to the total number of consecutive failed authentication attempts for a specific, valid user identity to the CS. Using invalid user identities or switching between valid user identities should not reset the cumulative count(s). The user should be locked out until an administrator reconfigures the CS. The defined number of unsuccessful authentication attempts may be different for the RUs than for the CS, and should be a positive integer.

Locking a user out from one RU should not impact that user's ability to access another RU. It should also not impact the user's ability to administer the CS from another RU or from the backside network.

FIA_AFL.1$_{(RU)}$ Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when an administrator-configurable number unsuccessful authentication attempts occur related to cumulative authentication failures of a specific user identity to an RU.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall lock the user out from future successful authentication to that RU.

Note: FIA_AFL.1.1 refers to the total number of consecutive failed authentication attempts for a specific, valid user identity to a RU. Using invalid user identities or switching between valid user identities should not reset the cumulative count(s). The user should be locked out until an administrator reconfigures the RU. The defined number of unsuccessful authentication attempts may be different for the RUs than for the CS, and should be a positive integer.

FIA_ATD.1$_{(SYS)}$ User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: remote user identities and enclave session identifiers.

FIA_UAU.2$_{(SYS)}$ User authentication before any action

FIA-UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Note: Network traffic that flows through a CS to an RU partition shall be considered to be performed on behalf of the user at the RU.

FIA_UAU.3$_{(SYS)}$ Unforgeable Authentication

FIA_UAU.3.1 The TSF shall prevent use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall prevent use of authentication data that has been copied from any other user of the TSF.

Note: The intention of this requirement is that an authentication mechanism that checks for the possession of a difficult to forge token, such as a FORTEZZA card, together with information that binds the possession of the token to its owner, such as a PIN, would be adequate unforgeability as long as the token has reasonable protection against fabrication of the binding information. For example, if the token locked itself after some number of failed attempts to match the binding information.

FIA_UAU.6$_{(RU)}$ Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions when TSF-initiated session locking is triggered.

Note: See requirement FTA_SSL.1$_{(RU)}$ as a reference for TSF-initiated session locking.

FIA_UAU.7$_{(SYS)}$ Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only acknowledgment of data entry to the user while the authentication is in progress.

Note: The authentication data that is provided by direct user entry shall not be displayed. In particular, if the user is required to enter a PIN at a keyboard for smartcard authentication, then the PIN should not be displayed, but it would be acceptable (desirable) to display a positive acknowledgment of each keystroke.

FIA_UID.2$_{(SYS)}$ User Identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Note: The TOE is not in a definable state until after a user powers the RU on. The user must authenticate to the RU before retrieving data or connecting to the CS. User "identity" is interpreted as "unique identity."

FIA_USB.1$_{(CS)}$ User-Subject Binding

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Note: In some architectures this requirement might result in the user at an RU having to re-authenticate to the CS. The only attributes that we have explicitly identified are the user identity and session identifier.

FMT_MOF.1$_{(SYS)}$ Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to determine and modify the behaviour of the functions listed in Table FMT_MOF.1 to an administrator role.

Table FMT_MOF.1- Managed security functions

Component	Management Function
FAU_ARP.1$_{(RU)}$	Adding, removing, or modifying alarms.
FAU_SAA.1$_{(CS)}$	Adding, modifying, or deleting rules from the set of rules that define potential violations.
FAU_SAA.3$_{(RU)}$	Deleting or generating the checksums used for cryptographic hashes of RU configuration data. Modifications to the BIOS and BIOS-based tests.
FAU_STG.4$_{(CS)}$	Deleting, modifying, or adding actions to be taken in case of audit storage failure.
FCS_CKM.1$_{(SYS)}$ FCS_CKM.3$_{(SYS)}$ FCS_CKM.4$_{(SYS)}$	Managing changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).
FDP_IFF.1$_{(CS)}$ FDP_IFF.1$_{(SYS)}$	Managing the attributes used to make explicit access based decisions.
FDP_ITT.2$_{(SYS)}$ FDP_ITT.3$_{(SYS)}$	N/A: These are functions are not configurable for the TOE.

Table FMT_MOF.1- Managed security functions

Component	Management Function
FDP_RIP.2$_{(SYS)}$	Performing residual information protection of the RU within the secure enclave.
FIA_AFL.1$_{(CS)}$ FIA_AFL.1$_{(RU)}$	Managing changes to the threshold for unsuccessful authentication attempts. Managing the locking and unlocking user accounts.
FIA_ATD.1$_{(SYS)}$	N/A: The administrator cannot define additional security attributes.
FIA_UAU.2$_{(SYS)}$	Managing authentication data.
FIA_UAU.6$_{(SYS)}$	N/A: The administrator cannot request re-authentication.
FIA_UID.2$_{(SYS)}$	Managing user identities.
FIA_USB.1$_{(CS)}$	Defining default subject security attributes.
FMT_MOF.1$_{(SYS)}$	N/A: Only a single role (administrators) can interact with TSF functions.
FMT_MSA.3$_{(SYS)}$	Managing the administrator accounts on the CS. Managing user identities (e.g., certificates) that allow sessions between the CS and an RU.
FMT_MTD.1$_{(SYS)}$	N/A: Only a single role (administrators) can interact with TSF functions.
FMT_REV.1$_{(SYS)}$	Managing the list of user identities for which revocation is possible.
FMT_SAE.1$_{(CS)}$	Managing actions to be taken if the expiration time for user identities has passed.
FMT_SMR.1$_{(SYS)}$	Managing the groups of individuals that are authorized users and/or administrators.
FPT_ITT.2$_{(SYS)}$	Management of the types of modification against which the TSF should protect. Managing the mechanism used to provide the protection of the data in transit between different parts of the TSF. Managing the separation mechanism.
FPT_ITT.3$_{(SYS)}$	Managing the types of modification against which the TSF should protect. Managing the mechanism used to provide the protection of the data in transit between different parts of the TSF. Management of the types of modification of TSF data the TSF should try to detect. Management of the actions that will be taken.
FPT_RPL$_{(SYS)}$	N/A: Replay shall be detected for all user identities and there is only a single action in the case of replay, which never varies.
FPT_STM.1$_{(CS)}$	Managing the system time setting.
FTA_SSL.1$_{(RU)}$	Specifying the time of user inactivity after which lock-out occurs. Specifying the default time of user inactivity after which lock-out occurs. Managing the events that should occur prior to unlocking the session.
FTA_TAB.1$_{(SYS)}$	Maintaining the text of banner.

Note: Table FMT_MOF.1 lists security management functions which are explicitly required by this component. Items suggested by the CC that are not applicable for this PP are indicated by an “N/A,” followed by a reason for why that management

function is not applicable. A combination of mechanisms (e.g., access controls and/or automated support tools) may be implemented to provide the capabilities called for in this component. Replay attacks (see FPT_RPL.$1_{(SYS)}$) is always detected, so the default behavior does not need management.

FMT_MSA.$1_{(SYS)}$ Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the P.SEPARATE and P.RECEIVE policies to restrict the ability to change_default, query, modify, or delete the security attributes of user identity and session identifiers to administrators.

Note: The P.SEPARATE policy is defined for the FDP_IFC.$1_{(CS)}$ and FDP_IFF.$1_{(CS)}$ components, while the P.RECEIVE policy is defined for the FDP_IFC.$1_{(SYS)}$ and FDP_IFF.$1_{(SYS)}$ components. System administrators must support these policies while managing the system's security attributes.

FMT_MSA.$2_{(SYS)}$ Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Note: User identities may be based on a complex representation (e.g., cryptographic certificates) within the system. This component requires that the format and content of this representation are secure with respect to the implementation the system. For instance, some certificate values might be unsafe for some cryptographic algorithms.

FMT_MSA.$3_{(SYS)}$ Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the P.SEPARATE and P.RECEIVE policies to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the administrator to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.$1_{(SYS)}$ Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to change_default, query, modify, delete, or clear the

a) specification of user identities,

b) specification of valid RU-to-CS connections,
c) specification of valid CU-to-RU connections,
d) specification of authorized RU peripheral devices, and
e) [ST assignment: list of other TSF data]
to administrators.

Note: All operations on TSF data is restricted to system administrators. Authorized users will have a defined user identity, that could be defined in varied implementations (e.g., a list of certificates or in a database). The specifications of TSF data listed are the minimum set. The list indicates what specifications of TSF data must be controlled to support the P.RECEIVE and P.SEPARATE policies.

FMT_REV.1$_{(SYS)}$ Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to administrators.

FMT_REV.1.2 The TSF shall enforce the rules immediate revocation of user identities and [ST assignment: other revocation rules].

Note: A minimal implementation mechanism must provide an “immediate” revocation function. Subsequent attempts to access the TOE by a revoked identity should fail. Other, flexible revocation functions (e.g., immediate session termination) may also be desirable, depending upon the end user’s needs.

FMT_SAE.1$_{(CS)}$ Time-limited authorization

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for user identities to administrators.

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to deny TOE access after the expiration time for the indicated security attribute has passed.

Note: User identities may be based on a complex representation (e.g., cryptographic certificates) within the system. The only required capability is to deny access to the TOE for users with expired identities.

FMT_SMR.1$_{(SYS)}$ Security roles

FMT_SMR.1.1 The TSF shall maintain the roles of administrator and authorized users.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Note: Other role definitions are desirable but are not required. In some cases it will be appropriate for administrators to be users of the system, but it should be easy to distinguish when they are acting as administrators from when they are acting as authorized users. Authorized users may potentially administer the CS by direct connection to the CS, via remote access from an RU, or via remote access from the back-side network.

FPT_FLS.1$_{(CS)}$ Failure with preservation of secure state.

FPT_FLS.1.1. The TSF shall preserve a secure state when the following types of failures occur:

a. The abstract machine fails or is turned off.
b. The TOE crashes.

Note: An abstract machine consists of the hardware, microcode, software, etc. on top of which the TOE runs. A secure state is one in which all open remote connections have been properly identified and authenticated, and all enclave sessions established with the CS correspond to an open remote connection. If there are no open connections or enclave sessions, the state is vacuously secure.

FPT_FLS.1$_{(RU)}$ Failure with preservation of secure state.

FPT_FLS.1.1. The TSF shall preserve a secure state when the following types of failures occur:

a. The abstract machine fails or is turned off.
b. The TOE crashes.
c. The user identity is voided.
d. The user activates the emergency shutdown procedure.

Note: A secure state is one in which no classified or sensitive information is available and that does not have an open connection with the enclave. A user identity may be automatically voided, for instance, when an authentication token is removed from the RU. The “failure” indicated by an emergency shutdown procedure indicates an emergency situation in the user environment. The procedure itself may be a special key sequence or combination.

FPT_ITT.2$_{(SYS)}$ TSF data transfer separation.

FPT_ITT.2.1. The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.

FPT_ITT.2.2. The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.

Note: Because the focus of this PP is that of a system, it is possible to consider the case where the system is composed of two or more independent systems (or products) corresponding to the CS and the RU. Before integration of the TOE, the FPT_ITT.2 component would be interpreted as a requirement for FPT_ITC.1 upon each of the independent units.

FPT_ITT.3$_{(SYS)}$ TSF data integrity monitoring.

FPT_ITT.3.1. The TSF shall be able to detect modification of data, substitution of data, and deletion of data for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2. Upon detection of a data integrity error, the TSF shall take the following actions: discard the affected data.

Note: Because the focus of this PP is that of a system, it is possible to consider the case where the system is composed of two or more independent systems (or products) corresponding to the CS and the RU. Before integration of the TOE, the FPT_ITT.3 component would be interpreted as a requirement for FPT_ITI.1 upon each of the independent units.

FPT_RPL.1$_{(SYS)}$ Replay detection.

FPT_RPL.1.1. The TSF shall detect replay for the following entities: messages sent between the RU and the CS.

FPT_RPL.1.2. The TSF shall perform deletion of repeated messages when replay is detected.

FPT_RVM.1$_{(SYS)}$ Non-bypassability of the TSP.

FPT_RVM.1.1. The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1$_{(SYS)}$ TSF domain separation.

FPT_SEP.1.1. The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2. The TSF shall enforce separation between the security domains of subjects in the TSC.

Note: The CS has no untrusted subjects.

FPT_STM.1$_{(CS)}$ Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Note: The time stamp mechanism may be integrated with the audit generation mechanism.

FTA_SSL.1$_{(RU)}$ TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session after a time interval of user inactivity by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: reauthentication of the user to the RU.

Note: The administrator should configure time intervals for inactivity time-outs based on considerations of risk versus mission criticality. Time-outs may be different for each RU in the system. The ST author should carefully define what constitutes "inactivity" for the TOE. For instance, remote users may be active on the RU while no data is being sent to the CS. Depending upon implementation choices and functional trade-offs, this scenario could be reasonably described as either an active, or inactive, user. It is important that the ST defines exactly what situations will cause session locking. In general, it is preferable for user inactivity to be closely associated with inactivity of the remote user at the RU (i.e., higher-level protocols on the RU).

FTA_TAB.1$_{(SYS)}$ Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Note: The contents of the advisory warning message should be configurable by the administrator.

5.2 ASSURANCE REQUIREMENTS

61 This Protection Profile (PP) specifies assurance requirements for each independent partition separately. It does not define an assurance level for the system as a whole. The assurance security requirements for both of the independent partitions happen to compose the same assurance level, EAL5. The assurance requirements are taken from Part 3 of the CC. The details of assurance requirements are listed only once; however, Application Notes for each independent partition are listed separately.

62 EAL5 is summarized in the following table.

Table 5.3 - Assurance Requirements for the CS and MU partitions: EAL5

Assurance class	Assurance Components	
Configuration management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.3	Development tools CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.3	Semiformal functional specification
	ADV_HLD.3	Semiformal high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_INT.1	Modularity
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.2	Semiformal correspondence demonstration
	ADV_SPM.3	Formal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.2	Standardized life-cycle model
	ALC_TAT.2	Compliance with implementation standards

Table 5.3 - Assurance Requirements for the CS and MU partitions: EAL5

Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_CCA.1	Covert channel analysis
	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.3	Moderately resistant

63

ACM_AUT.1 Partial CM automation

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_CAP.4 Generation support and acceptance procedures

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labelled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.3 Development tools CM coverage

ACM_SCP.3.1D The developer shall provide CM documentation.

ACM_SCP.3.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, security flaws, and development tools and related information.

ACM_SCP.3.2C The CM documentation shall describe how configuration items are tracked by the CM system.

ACM_SCP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_DEL.2 Detection of modification

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Note: If FAU_ARP.$1_{(MU)}$ is implemented as a start-up function, the documented procedures should include instructions for how to recover from an authorised modification to the MU's configuration data.

ADV_FSP.3 Semiformal functional specification

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.1C The functional specification shall describe the TSF and its external interfaces using a semiformal style, supported by informal, explanatory text where appropriate.

ADV_FSP.3.2C The functional specification shall be internally consistent.

ADV_FSP.3.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.3.4C The functional specification shall completely represent the TSF.

ADV_FSP.3.5C The functional specification shall include rationale that the TSF is completely represented.

ADV_FSP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.3 Semiformal high-level design

ADV_HLD.3.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.3.1C The presentation of the high-level design shall be semiformal.

ADV_HLD.3.2C The high-level design shall be internally consistent.

ADV_HLD.3.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.3.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.3.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.3.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.3.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.3.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing complete details of all effects, exceptions and error messages.

ADV_HLD.3.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.3.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_IMP.2 Implementation of the TSF

ADV_IMP.2.1D The developer shall provide the implementation representation for the entire TSF.

ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C The implementation representation shall be internally consistent.

ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

ADV_IMP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.2.2E The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

ADV_INT.1 Modularity

ADV_INT.1.1D The developer shall design and structure the TSF in a modular fashion that avoids unnecessary interactions between the modules of the design.

ADV_INT.1.2D The developer shall provide an architectural description.

ADV_INT.1.1C The architectural description shall identify the modules of the TSF.

ADV_INT.1.2C The architectural description shall describe the purpose, interface, parameters, and effects of each module of the TSF.

ADV_INT.1.3C The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

ADV_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_INT.1.2E The evaluator shall determine that both the low-level design and the implementation representation are in compliance with the architectural description.

ADV_LLD.1 Descriptive low-level design

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.2 Semiformal correspondence demonstration

ADV_RCR.2.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.2.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.2.2C For each adjacent pair of provided TSF representations, where portions of both representations are at least semiformally specified, the demonstration of correspondence between those portions of the representations shall be semiformal.

ADV_RCR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_SPM.3 Formal TOE security policy model

ADV_SPM.3.1D The developer shall provide a TSP model.

ADV_SPM.3.2D The developer shall demonstrate or prove, as appropriate, correspondence between the functional specification and the TSP model.

ADV_SPM.3.1C The TSP model shall be formal.

ADV_SPM.3.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.3.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.3.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.3.5C Where the functional specification is semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal.

ADV_SPM.3.6C Where the functional specification is formal, the proof of correspondence between the TSP model and the functional specification shall be formal.

ADV_SPM.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ADM.1 Administrator guidance

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Note: If $FAU\_ARP.1_{(MU)}$ is implemented as a start-up function, the user documentation should include instructions for the MU user as to the meaning of the alarm and what procedures the user should carry out in the event of an alarm.

ALC_DVS.1 Identification of security measures

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_LCD.2 Standardised life-cycle model

ALC_LCD.2.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.2.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.2.3D The developer shall use a standardised life-cycle model to develop and maintain the TOE.

ALC_LCD.2.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.2.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.2.3C The life-cycle definition documentation shall explain why the model was chosen.

ALC_LCD.2.4C The life-cycle definition documentation shall explain how the model is used to develop and maintain the TOE.

ALC_LCD.2.5C The life-cycle definition documentation shall demonstrate compliance with the standardised life-cycle model.

ALC_LCD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.2 Compliance with implementation standards

ALC_TAT.2.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.2.2D The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.2.3D The developer shall describe the implementation standards to be applied.

ALC_TAT.2.1C All development tools used for implementation shall be well-defined.

ALC_TAT.2.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.2.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.2.2E The evaluator shall confirm that the implementation standards have been applied.

ATE_COV.2 Analysis of coverage

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.2 Testing: low-level design

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA_MSU.2 Validation of analysis

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE security function evaluation

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.3 Moderately resistant

AVA_VLA.3.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.3.2D The developer shall document the disposition of identified vulnerabilities.

AVA_VLA.3.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.3.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.3.3C The evidence shall show that the search for vulnerabilities is systematic.

AVA_VLA.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.3.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.3.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.3.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.3.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

5.3 ENVIRONMENTAL SECURITY REQUIREMENTS

64 The environmental security requirements assumed in this PP are summarized in Table 5.4. The requirements levied on the environment are expected to be enforced through accreditation and certification of the TOE and through operational procedures enforced by enclave staff.

Table 5.4 - Environmental security requirements

IT Environment	Non-IT Environment
FAU_ARP.1$_{(ENV)}$	ACCREDIT$_{(ENV)}$
FAU_SAA.1$_{(ENV)}$	ADMIN$_{(ENV)}$
FAU_SAR.1$_{(ENV)}$	AUTHORIZED$_{(ENV)}$
FAU_SAR.2$_{(ENV)}$	CLEARED$_{(ENV)}$
FAU_SAR.3$_{(ENV)}$	CONNECT$_{(ENV)}$
FCS_CKM.1$_{(ENV)}$	DUE_CARE$_{(ENV)}$
FCS_CKM.4$_{(ENV)}$	INSTALL$_{(ENV)}$
FMT_MSA.2$_{(ENV)}$	ISOLATION$_{(ENV)}$
	PERIPHERALS$_{(ENV)}$
	PHYSICAL$_{(ENV)}$
	RESPONSE$_{(ENV)}$
	REVIEW$_{(ENV)}$
	SINGLE_USER$_{(ENV)}$
	TRAINING$_{(ENV)}$

65 It is possible that the system implementing the TOE will include features that are capable of satisfying the IT Environment requirements. For each case where the TOE implements an IT Environment requirement, those features are considered a part of the TOE and are subect to the same assurance requirements that apply to the rest of the TOE.

66

5.3.1 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

67 The following requirements apply to the CS IT environment. The components are modeled off CC components. The term “TSF” has been refined to say “TOE Environment.” This “refinement” is done to avoid confusion with using the same term it two different contexts. It is not an invalid refinement with respect to the CC,

because the intent of valid refinement is not violated and because CC restrictions do not extend strictly to components in the IT environment.

FAU_ARP.1$_{(ENV)}$ Security alarms

FAU_ARP.1.1 The TOE environment shall take an alarm action to alert an administrator of the CS upon detection of a potential security violation.

FAU_SAA.1$_{(ENV)}$ Potential violation analysis

FAU_SAA.1.1 The TOE environment shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TOE environment's security policy.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of failed I&A or other intrusion attempts known to indicate a potential security violation.

FAU_SAR.1$_{(ENV)}$ Audit review

FAU_SAR.1.1 The TOE environment shall provide administrators with the capability to read all data from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2$_{(ENV)}$ Restricted audit review

FAU_SAR.2.1 The TOE environment shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3$_{(ENV)}$ Selectable audit review

FAU_SAR.3.1 The TOE environment shall provide the ability to perform searches, sorting, and ordering of audit data based on date and time of the event, type of event, user identity, event success or failure criteria, and session identifier.

FCS_CKM.1$_{(ENV)}$ Cryptographic Key Generation

FCS_CKM.1.1 The TOE environment shall generate cryptographic keys for the RU media encryption mechanism and the RU/CS device authentication mechanism in accordance with a Type I cryptographic key generation algorithm and Type I cryptographic key sizes.

FCS_CKM.4$_{(ENV)}$ Cryptographic Key Destruction

FCS_CKM.4.1 The TOE environment shall destroy cryptographic keys for the RU media encryption mechanism and the RU/CS device authentication mechanism in accordance with Type I cryptographic key destruction methods.

FMT_MSA.2$_{(ENV)}$ Secure security attributes

FMT_MSA.2.1 The TOE environment shall ensure that only secure values are accepted for security attributes.

5.3.2 SECURITY REQUIREMENTS FOR THE NON-IT ENVIRONMENT

Table 5.5 - Security Requirements for the Non-IT Environment

Identifier	Description
$ACCREDIT_{(ENV)}$	The facility and TOE must receive formal accreditation to process SECRET information, and all information is implicitly marked and handled as such.
$ADMIN_{(ENV)}$	At least one administrator will be assigned to administer the system. For larger systems, an appropriate number of administrators will be assigned.
$AUTHORIZED_{(ENV)}$	TOE administrators will grant access to the TOE only to users and administrators who have a need-to-know for the type of information managed by the TOE.
$CLEARED_{(ENV)}$	Authorized users and administrators of the TOE will be cleared to a level appropriate to the sensitivity of the user data on the system.
$CONNECT_{(ENV)}$	The authorized user of the RU will attempt to connect only to authorized CSs.
$DUE\_CARE_{(ENV)}$	The authorized user of the RU must not operate the RU in hazardous or insecure settings. The authorized user of the RU must not attempt to reconfigure the system or to perform other unauthorized administrative actions. The authorized user of the RU will shut down the RU properly and store it securely while it is not in use. Authorized users must exercise due care when importing software to execute on the RU.
$INSTALL_{(ENV)}$	The TOE will be delivered and installed in a manner that maintains system security.
$ISOLATION_{(ENV)}$	The CS is physically isolated from authorized users, so that only administrators can physically access it.
$PERIPHERALS_{(ENV)}$	Only authorized peripherals will be attached to the CS and RU.
$PHYSICAL_{(ENV)}$	Appropriate physical controls will be used to protect the enclave.
$RESPONSE_{(ENV)}$	Administrators will be available to respond to security alarms during operation of the TOE. Response procedures will be effective to a measure commensurate with the risks associated with unauthorized access to the information within the TOE.
$REVIEW_{(ENV)}$	Administrators will review audit records periodically, with the frequency of reviews to be determined by the responsible authorities of the enclave.
$SINGLE\_USER_{(ENV)}$	Only a single authorized user will use the RU while connected to a given CS. Only processes belonging to the authenticated user operate in the RU and each process is authorized to access all information on the RU.
$TRAINING_{(ENV)}$	Authorized users and administrators of the TOE will receive appropriate training in the secure operation of the TOE. Training will include appropriate procedures to prevent unauthorized or unwitting export of sensitive information from the TOE.

6 RATIONALE

68 This section provides a set of rationale arguments for the PP.

- Section 6.1 addresses Objectives coverage of Assumptions, Threats, and Policies.
- Section 6.2 addresses Requirements coverage of Objectives.
- Section 6.3 addresses the adequacy of the assurance requirements chosen for this PP.
- Section 6.4 addresses the minimum “strength of function” issues for this PP.
- Section 6.5 addresses the Dependency coverage for this PP.
- Section 6.6 addresses the comprehensive argument that the PP’s IT requirements “form a mutually supportive and internally consistent whole.”

6.1 ASSUMPTION, THREAT, AND POLICY COVERAGE

69 This section contains two subsections, one to address the coverage of Assumption statements and a second to address coverage of Policy and Threat statements. Each subsection provides a mapping table and individual arguments for the coverage of individual environmental statement. For Policy and Threat statements, Assumptions are used as part of the coverage argument, allowing Assumption-covering objectives to be referenced indirectly.

6.1.1 ASSUMPTION COVERAGE

70 Table 6.1 lists the Assumption statements and maps the environmental objectives that cover each statement. Following this table are individual arguments for the coverage of each Assumption. Coverage of Assumptions is determined with respect to mapped Environmental Objectives only.

Table 6.1 - Assumption Coverage

Assumptions	Environmental Objectives	
$A.CONTROLLED_{(RU)}$	$OE.OPERATE_{(RU)}$	$OE.ADMIN_{(SYS)}$
	$OE.INSTALL_{(SYS)}$	$OE.PHYSICAL_{(SYS)}$
$A.DEDICATED_{(CS)}$	$OE.ADMIN_{(SYS)}$	$OE.INSTALL_{(SYS)}$
$A.FACILITY_{(CS)}$	$OE.ACCREDITED_{(SYS)}$	$OE.PHYSICAL_{(SYS)}$
$A.TRUSTED\_ADMIN_{(SYS)}$	$OE.CLEARED_{(SYS)}$	$OE.TRAINED_{(SYS)}$
$A.TRUSTED\_USER_{(SYS)}$	$OE.CLEARED_{(SYS)}$	$OE.TRAINED_{(SYS)}$

A.CONTROLLED$_{(RU)}$ Configuration and administration of the RU are duties performed by TOE administrators.

71 Administrative actions on the RU are only authorized for administrators (OE.OPERATE$_{(RU)}$). OE.PHYSICAL$_{(SYS)}$ provides for a measure of physical protection of the RU, to reduce the risk that its configuration will be altered by malicious agents. Installation, configuration, and other administration duties are explicit responsibilities of (only) the authorized administrators (OE.ADMIN$_{(SYS)}$ and OE.INSTALL$_{(SYS)}$).

A.DEDICATED$_{(CS)}$ The CS is a dedicated communications server and does not support general-purpose accounts or applications for individuals other than the designated administrators of the CS.

72 The use of the CS is controlled by administrators of the TOE (OE.ADMIN$_{(SYS)}$) and is dependent on how they install the TOE (OE.INSTALL$_{(SYS)}$).

A.FACILITY$_{(CS)}$ The CS operates within a protected facility that provides protection against unauthorized physical access.

73 Formal accreditation for the enclave facility to operate the TOE (OE.ACCREDITED$_{(SYS)}$) ensures that the organization believes it is appropriate for the facility to use the TOE for processing sensitive information. Typically, the accreditation process will identify operational vulnerabilities and formally acknowledge an acceptable level of residual risk. The facility must provide physical protection of the TOE (OE.PHYSICAL$_{(SYS)}$).

A.TRUSTED_ADMIN$_{(SYS)}$ Administrators will not deliberately abuse their privileges so as to violate organizational security policies and are competent to manage the TOE and the information it contains.

74 Trust in the administrators is increased by formally clearing those individuals (OE.CLEARED$_{(SYS)}$) and providing them adequate training (OE.TRAINED$_{(SYS)}$).

A.TRUSTED_USER$_{(SYS)}$ Authorized users of the RU will not intentionally violate organizational security policies and will exercise due care in the operation and use of the RU.

75 Trust in the authorized users is increased by formally clearing those individuals (OE.CLEARED$_{(SYS)}$) and providing them adequate training (OE.TRAINED$_{(SYS)}$).

6.1.2 POLICY AND THREAT COVERAGE

76 Table 6.2 lists either the Policy or Threat statement that requires coverage in the first column. Relevant assumptions are listed in the second column. Assumptions are relevant if they support the Policy or mitigate a Threat. The use of an Assumption in the coverage argument infers the use of the Objectives that support the Assumption. TOE Objectives that cover each Policy and Threat are listed in the third column.

Finally, Environmental Objectives that cover each Policy and Threat are listed in the fourth column. Following this table are individual arguments for the coverage of each Policy and Threat statement. Coverage is determined with respect to all mapped Assumptions, TOE Objectives, and Environmental Objectives for each Policy and Threat.

Table 6.2 - Policy and Threat Coverage

Policy/Threat	Assumptions	TOE Objectives	Environment Objectives
P.ACCOUNT	A.TRUSTED_ADMIN$_{(SYS)}$ A.DEDICATED$_{(CS)}$ A.FACILITY$_{(CS)}$	O.AUDIT$_{(SYS)}$ O.BANNER$_{(SYS)}$ O.IDENTIFY$_{(SYS)}$	OE.AUDIT$_{(CS)}$
P.CONFIDENTIALITY	A.FACILITY$_{(CS)}$ A.TRUSTED_ADMIN$_{(SYS)}$ A.TRUSTED_USER$_{(SYS)}$	O.ACCESS$_{(SYS)}$ O.IDENTIFY$_{(SYS)}$ O.MEDIA$_{(RU)}$ O.NO_EAVESDROP$_{(SYS)}$ O.RECEIVE$_{(SYS)}$	OE.CRYPTOKEYS$_{(SYS)}$
P.ELGIBLE	A.TRUSTED_ADMIN$_{(SYS)}$ A.TRUSTED_USER$_{(SYS)}$	O.ACCESS$_{(SYS)}$ O.MEDIA$_{(RU)}$ O.NO_EAVESDROP$_{(SYS)}$	OE.PHYSICAL$_{(SYS)}$.
P.EXPORT	A.FACILITY$_{(CS)}$ A.TRUSTED_ADMIN$_{(SYS)}$ A.TRUSTED_USER$_{(SYS)}$	O.MEDIA$_{(RU)}$ O.NO_EAVESDROP$_{(SYS)}$ O.RECEIVE$_{(SYS)}$	OE.ACCREDITED$_{(SYS)}$ OE.CRYPTOKEYS$_{(SYS)}$
P.INTEGRITY	A.FACILITY$_{(CS)}$ A.TRUSTED_ADMIN$_{(SYS)}$ A.TRUSTED_USER$_{(SYS)}$	O.ACCESS$_{(SYS)}$ O.DETECT$_{(RU)}$ O.IDENTIFY$_{(SYS)}$ O.RECEIVE$_{(SYS)}$	OE.CRYPTOKEYS$_{(SYS)}$
P.MANAGE	A.CONTROLLED$_{(RU)}$ A.TRUSTED_ADMIN$_{(SYS)}$	O.MANAGE$_{(SYS)}$	OE.INSTALL$_{(SYS)}$ OE.TRAINED$_{(SYS)}$
P.MARKING	A.FACILITY$_{(CS)}$ A.TRUSTED_USER$_{(SYS)}$ A.TRUSTED_ADMIN$_{(SYS)}$		OE.CLEARED$_{(SYS)}$ OE.TRAINED$_{(SYS)}$
T.ALTER	A.FACILITY$_{(CS)}$ A.TRUSTED_ADMIN$_{(SYS)}$ A.TRUSTED_USER$_{(SYS)}$	O.DETECT$_{(RU)}$	OE.OPERATE$_{(RU)}$ OE.PHYSICAL$_{(SYS)}$

Table 6.2 - Policy and Threat Coverage

Policy/Threat	Assumptions	TOE Objectives	Environment Objectives
T.CAPTURE		O.NO_EAVESDROP$_{(SYS)}$ O.RECEIVE$_{(SYS)}$ O.SELF-PROTECT$_{(SYS)}$	OE.OPERATE$_{(RU)}$ OE.PHYSICAL$_{(SYS)}$ OE.CRYPTOKEYS$_{(SYS)}$
T.CRASH		O.SELF-PROTECT$_{(SYS)}$	
T.ERROR	A.TRUSTED_ADMIN$_{(SYS)}$ A.TRUSTED_USER$_{(SYS)}$	O.DETECT$_{(RU)}$ O.RECEIVE$_{(SYS)}$ O.MEDIA$_{(RU)}$	OE.CRYPTOKEYS$_{(SYS)}$
T.IMPORT	A.DEDICATED$_{(CS)}$	O.DETECT O.SELF-PROTECT	OE.INSTALL$_{(SYS)}$ OE.OPERATE$_{(RU)}$ OE.TRAINED
T.INTRUDE		O.ACCESS$_{(SYS)}$ O.RECEIVE$_{(SYS)}$ O.DETECT$_{(RU)}$ O.IDENTIFY $_{(SYS)}$ O.MEDIA$_{(RU)}$	OE.OPERATE$_{(RU)}$ OE.PHYSICAL$_{(SYS)}$ OE.CRYPTOKEYS$_{(SYS)}$
T.MASQUERADE		O.IDENTIFY$_{(SYS)}$	
T.PHYSICAL	A.DEDICATED$_{(CS)}$ A.FACILITY$_{(CS)}$	O.DETECT$_{(RU)}$ O.IDENTIFY$_{(SYS)}$	OE.CLEARED$_{(SYS)}$ OE.OPERATE$_{(RU)}$ OE.PHYSICAL$_{(SYS)}$
T.TRAFFIC		O.NO_EAVESDROP$_{(SYS)}$	OE.OPERATE$_{(RU)}$

77

P.ACCOUNT User activity shall be monitored to the extent that sanctions can be applied when malfeasance occurs, and to ensure that system controls are properly applied.

78 Users are required to be identified and authenticated by the O.IDENTIFY$_{(SYS)}$ objective. Upon accessing the TOE, users are made cognizant that they are entering a government computer system through O.BANNER$_{(SYS)}$. Once access to the TOE has been established, the O.AUDIT$_{(SYS)}$ objective requires an audit trail to be kept for user activity, and to allow association of user actions with identified individuals. Finally, the OE.AUDIT$_{(SYS)}$ objective provides audit review capabilities and requires administrators to perform reviews periodically, so that the audit trails are used effectively. OE.AUDIT$_{(SYS)}$ also requires administrators to respond effectively to any alarms that the TOE generates. A.TRUSTED_ADMIN$_{(SYS)}$ assumes that

administrators are competent to determine malfeasance from observation of user behavior on the system, and that they take appropriate actions when malfeasance is detected. This assumption also assumes that system functions supporting these objectives will be competently managed.

79 Allocating the audit review capabilities to the IT environment ($OE.AUDIT_{(CS)}$) requires justification. The CS provides limited functionality ($A.DEDICATED_{(CS)}$) and exists within an accredited facility that has established capabilities for user accountability ($A.FACILITY_{(CS)}$). There is a relatively narrow focus of accountability concerns that are added to those that preexist in the enclave environment. The major concerns are failed I&A attempts and other "penetration" activities from outside the enclave.[1] This narrow focus of accountability concerns generally simplifies necessary mechanisms required for audit review in the enclave environment. Because there are preexisting and comprehensive accountability concerns there, and the TOE adds relatively simple concerns to those, it is appropriate to levy the audit review requirements to the enclave environment.

P.CONFIDENTIALITYThe confidentiality of user data must be protected.

80 All individuals using the system are uniquely identified and authenticated ($O.IDENTIFY_{(SYS)}$), thus allowing accountability for access to data. For data subject to the enclave security policy, that policy as defined for the accountable individual, including disclosure, is enforced ($O.ACCESS_{(SYS)}$). For data being transferred using the COMM, the TOE prevents disclosure to eavesdroppers with a strength appropriate to the data ($O.NO\_EAVESDROP_{(SYS)}$). The only channels from the data on a RU are to the authenticated user, who does not intentionally violate organizational security policies ($A.TRUSTED\_USER_{(SYS)}$), and through the COMM to a mutually authenticated CS ($O.RECEIVE_{(SYS)}$); when the TOE is not operating, protected data is inaccessible ($O.MEDIA_{(RU)}$). Infrastructure support for the media encryption function on the RU is provided via $OE.CRYPTOKEYS_{(SYS)}$. Likewise, the CS is only accessible through the COMM to a mutually authenticated MU ($O.RECEIVE_{(SYS)}$), through the enclave, and with administrators who are trusted not to abuse their privileges ($A.TRUSTED\_ADMIN_{(SYS)}$); no unauthorized users have access to the enclave ($A.FACILITY_{(CS)}$).

P.ELGIBLE Authorized users and administrators of the TOE shall be eligible to access information that is collected, created, communicated, computed, disseminated, processed, or stored on the TOE.

81 This policy focuses on the eligibility of users to access the TOE. The policy is met by ensuring that all users and administrators of the TOE have an appropriate clearance level and training for the information handled by the TOE ($A.TRUSTED\_USER_{(SYS)}$ and $A.TRUSTED\_ADMIN_{(SYS)}$).

82 The TOE potentially extends the access of the TOE users to information that is collected, created, communicated, computed, disseminated, processed, or stored within the enclave. In other words, only authorized users and administrators of the

1. Some concerns are countered by the TOE's capability to generate alarms (see the FAU_SAA requirements).

protected enclave are eligible to access information that is collected, created, communicated, computed, disseminated, processed, or stored within the enclave. Compliance with that policy is extended to the TOE by restricting the access to information by TOE users to the information that is allowed to them on the protected enclave ($O.ACCESS_{(SYS)}$) and by protecting the information handled by the TOE from unauthorized disclosure by providing physical protection of the TOE hardware, software, documentation, and classified data ($OE.PHYSICAL_{(SYS)}$). The protection of data stored on the RU while it is not in use is provided by $O.MEDIA_{(RU)}$. The protection of the communications between the RU and the CS from eavesdropping and spoofing are provided by $O.NO\_EAVESDROP_{(SYS)}$ and $O.RECEIVE_{(SYS)}$, respectively.

P.EXPORT Authorized users and administrators of the TOE shall not export information processed by the TOE without proper and explicit authorization.

83 While the RU is not in use, its information is unattainable to unauthorized users through $O.MEDIA_{(RU)}$. Therefore, information cannot be exported from the RU without explicit actions by the remote user. Information is protected during transit between a RU and CS (or vice versa) by $O.NO\_EAVESDROP_{(SYS)}$. Spoofing of either partition into connecting to some untrusted system is prevented via $O.RECEIVE_{(SYS)}$. Infrastructure support for the CS/RU mutual authentication function is provided via $OE.CRYPTOKEYS_{(SYS)}$. User information is thereby protected outside of the enclave (during storage on the RU, transit, and connection establishment). The remainder of protection features to fulfill this policy comes from non-technical controls.

84 Users and administrators of the system are cleared, trained, and assumed to be observant of organizational security policies ($A.TRUSTED\_USER_{(SYS)}$ and $A.TRUSTED\_ADMIN_{(SYS)}$). The enclave environment is protected from access by unauthorized users who are not trusted to be observant of policies ($A.FACILITY_{(CS)}$). All information within the system is considered equally sensitive and implicitly marked ($OE.ACCREDITED_{(SYS)}$), reducing export errors by users by simplifying the process of determining information sensitivity. While these assumptions and environmental objectives do not provide rigorous coverage, they supplement each other and when used in conjunction with technical measures.

P.INTEGRITYThe integrity of user data must be protected.

85 All individuals using the system are uniquely identified and authenticated ($O.IDENTIFY_{(SYS)}$), thus allowing accountability for access to data. For data subject to the enclave security policy, that policy as defined for the accountable individual, including creation and modification of data, is enforced ($O.ACCESS_{(SYS)}$). For data being transferred using the COMM, the TOE detects and discards any data that does not originate from another CS or MU which are mutually authenticated ($O.RECEIVE_{(SYS)}$). The only channels to the data on a RU are from the authenticated user, who does not intentionally violate organizational security policies ($A.TRUSTED\_USER_{(SYS)}$), and through the COMM from a mutually authenticated CS ($O.RECEIVE_{(SYS)}$); infrastructure support for the CS/RU mutual authentication function is provided via $OE.CRYPTOKEYS_{(SYS)}$. When the TOE is not operating,

modifications to protected data can be detected ($O.DETECT_{(RU)}$). Likewise, the CS is only accessible through the COMM from a mutually authenticated MU ($O.RECEIVE_{(SYS)}$), through the enclave, and with administrators who are trusted not to abuse their privileges ($A.TRUSTED\_ADMIN_{(SYS)}$); no unauthorized users have access to it ($A.FACILITY_{(CS)}$).

P.MANAGE The TOE shall be managed such that its security functions are implemented and preserved throughout its operational lifetime.

86 This policy is primarily covered by requiring adequate management support via $O.MANAGE_{(SYS)}$, as well as trained, cleared, and competent administrators ($A.TRUSTED\_ADMIN_{(SYS)}$) who are adequately trained ($OE.TRAINED_{(SYS)}$) to manage the system in its operational environment. Authorized users do not perform administrative functions on the RU ($A.CONTROLLED_{(RU)}$).

87 $O.MANAGE_{(SYS)}$ applies to the TOE as a whole, as the management of security functions should be uniformly adequate, regardless of partition environment. Security attributes must be managed and assigned secure values, and the TOE must be configurable by administrators to support the system's security policies. Security functions that implement protection on the system must be managed by administrators. Administrators should be able to revoke access to the TOE, so that the TOE's policy enforcement can accurately reflect real-world changes in user authorizations. Adequate management of the TOE depends on proper installation of security enforcement and security management functions ($OE.INSTALL_{(SYS)}$).

P.MARKINGUser data must be adequately marked to describe the sensitivity of the information.

88 Coverage of P.MARKING relies strongly on assumptions and other environmental controls. Policy coverage through environmental assumptions may have some inherent weakness. However, for this particular policy, it is an unavoidable consequence of having an environment with uniform information sensitivity, because such environments usually do not employ automated labelling mechanisms. Such environments are a commonly accepted practice with well-understood trade-offs.

89 The fundamental assumption of implicit marking associated with $A.FACILITY_{(CS)}$ simply restates this common concept of operations; i.e., all information within the environment is to be protected as if it were marked at a specific information sensitivity (e.g., "SECRET-high"). $A.FACILITY_{(CS)}$ also assumes that the enclave environment has physical isolation that is appropriate for the information sensitivity. Only trusted users and administrators have logical access to the TOE and the enclave environment. Both users and administrators are trained to provide appropriate protection of SECRET data and are trusted to competently apply protective measures ($A.TRUSTED\_USER_{(SYS)}$ and $A.TRUSTED\_ADMIN_{(SYS)}$).

T.ALTER An unauthorized user may surreptitiously gain access to the TOE and attempt to alter and/or replace system elements (e.g., hardware, firmware, or software) in an attempt to subvert the device.

90 There will be environmental support for the TOE ($OE.PHYSICAL_{(SYS)}$) to provide protection against physical alterations of the system. This support is augmented by providing a mechanism to detect unauthorized changes to it's configuration ($O.DETECT_{(RU)}$) and $A.TRUSTED\_USER_{(SYS)}$ which places the RU under the control of a trusted user. The $A.FACILITY_{(CS)}$ assumption provides strong environmental controls for the prevention, detection, and recovery from physical alteration threats. Supplementing the protection under $A.FACILITY_{(CS)}$ is $A.TRUSTED\_ADMIN_{(SYS)}$, which assumes that competent system administrators will be observant of the CS in the enclave environment and therefore will be cognizant of unauthorized physical alterations. $OE.OPERATE_{(RU)}$ provides additional protection for the RU by requiring due care for the unit during storage, while it is not in the presence of the authorized user.

T.CAPTURE An agent may eavesdrop on, or otherwise capture, data being transferred on a communications channel.

91 $O.NO\_EAVESDROP_{(SYS)}$ protects the confidentiality of data within the COMM with mechanisms that are appropriate for SECRET-level information. $O.RECEIVE_{(SYS)}$ protects against unauthorized connections between CS and RU partitions, preventing spoofing attacks that might be initiated by a malicious host on the COMM that is intercepting connection set-up traffic. Infrastructure support for the CS/RU mutual authentication function is provided via $OE.CRYPTOKEYS_{(SYS)}$. The combination of $OE.PHYSICAL_{(SYS)}$ and $O.SELF\text{-}PROTECT_{(SYS)}$ protect against physical and penetration attacks (respectively) that undermine the implementation of $O.NO\_EAVESDROP_{(SYS)}$, which provides the protection of the communications channel. The authorized user of the RU is required to help counter this threat by connecting only to authorized CS units ($OE.OPERATE_{(RU)}$).

T.CRASH The TOE may take actions based on security-critical data that, due to interruption of the operation of the TOE, is either incomplete or corrupted.

92 If the operation of the TOE is interrupted, the TOE will protect its security-related functions against interference and tampering (O.SELF-PROTECT). It does this by dropping any affected connections, thus requiring connection establishment to be re-initiated from scratch, using complete and uncorrupted data.

T.ERROR A user may attempt to perform unauthorized or erroneous actions that will compromise user and/or system resources.

93 The threat of a user performing unauthorized or erroneous actions that will compromise user and/or system resources is addressed at the RU by $O.DETECT_{(RU)}$ which ensures that the RU will detect unauthorized changes to its configuration and $O.RECEIVE_{(SYS)}$ which ensures that a RU will only communicate with a CS with which it has mutually authenticated. Infrastructure support for the CS/RU mutual

authentication function is provided via $OE.CRYPTOKEYS_{(SYS)}$. $O.MEDIA_{(RU)}$ ensures that data stored on the RU will be protected while the unit is not being used in the TOE configuration. The risk of compromise of user or system resources is further reduced by the assumptions $A.TRUSTED\_USER_{(SYS)}$, which assumes that the users are trained and will not intentionally violate organizational security policies, and $A.TRUSTED\_ADMIN_{(SYS)}$, which assumes that the administrators are trained and will not deliberately abuse their privileges so as to violate security policies.

T.IMPORT An authorized user or administrator of the TOE may unwittingly introduce malicious code into the system, resulting in a compromise of the integrity and/or availability of user and/or system resources.

94 Authorized users and administrators are trained as to establishment and maintenance of sound security policies and practices ($OE.TRAINED_{(SYS)}$). The TOE protects its security relevant functions from tampering, including that of malicious code ($O.SELF\text{-}PROTECT_{(SYS)}$). The RU detects any unauthorized changes to its configuration, including that caused by malicious code ($O.DETECT_{(RU)}$). Also, the remote access system will be delivered, installed, managed, and operated in a manner that maintains system security ($OE.INSTALL_{(SYS)}$). Authorized users must exercise due care when importing software to execute on the RU ($OE.OPERATE_{(RU)}$). This threat is partially mitigated by $A.DEDICATED_{(CS)}$, which restricts the CS from serving as a general-purpose host with non-administrative users, and thereby reduces the chances that arbitrary software will be imported.

T.INTRUDE An unauthorized user may use the TOE to gain access to the secure enclave.

95 The threat of an unauthorized user making use of the TOE to gain access to the secure enclave is based on the fact that TOE provides an interface to the secure enclave that may be outside the normal physical and procedural controls of the secure enclave. With the exception of the CS interface to the COMM, the CS is located within the domain of physical control of the secure enclave. The CS is expected ($OE.PHYSICAL_{(SYS)}$) to be physically protected from intruder access within the secure enclave to the same extent as the rest of the enclave is protected. It is assumed that the strength of the authentication mechanisms that are used for the TOE are suitable for access to the enclave through the CS interface to the enclave boundary. $O.ACCESS_{(SYS)}$ ensures that an authenticated user only accesses information that would have been allowed within the protected enclave.

96 The threat of an intruder gaining access through the COMM interface, which is provided for RUs, is reduced by the security objective $O.RECEIVE_{(SYS)}$ which ensures that the CS only accepts connections by authorized RUs and that all of the connections that are accepted are subject to the TOE security requirements. By meeting the objective $O.RECEIVE_{(SYS)}$ the threat is restricted to the case of an intruder, directly or indirectly, gaining access to a RU that is actively connected to CS. However, $O.IDENTIFY_{(SYS)}$ ensures that an active connection of a RU to a CS requires that a valid user was properly identified and authenticated at the RU. $O.ACCESS_{(SYS)}$ ensures that the authenticated user only accesses information that would have been allowed within the protected enclave. Meeting the objectives $O.DETECT_{(RU)}$ and $O.MEDIA_{(RU)}$ protect against an intruder indirectly gaining

access to the enclave through the RU while OE.OPERATE$_{(RU)}$ ensures that the appropriate protections are in place, while the RU is both connected to the CS and when it is not in use. Depending upon the strength of controls in the RU environment, there is the residual risk that the physical protections for a connected RU could be breached and an intruder could gain access to the enclave through the connection.

T.MASQUERADE An unauthorized user may attempt to gain access to the TOE by pretending to be an authorized user.

97 The threat of an insider impersonating another authorized user of the system is addressed by the security objective O.IDENTIFY$_{(SYS)}$, which provides for authentication of users.

T.PHYSICAL Security-critical parts of the TOE may be subject to physical attack which may compromise security.

98 Protection against physical attacks are handled differently for the CS and RU components due to the difference in their threat environments. Authorized users of the RU are identified and authorized to use the TOE, as is similarly required for users of the TOE at the CS partition (O.IDENTIFY$_{(SYS)}$ and OE.CLEARED$_{(SYS)}$). Physical threats to the RU are partially mitigated by requiring the remote user to exercise due care in handling and operation of the RU (OE.OPERATE$_{(RU)}$) and detecting when a successful attack (i.e., by an outsider) modifies the RU configuration (O.DETECT$_{(RU)}$). Within the CS environment, additional controls are appropriate. A.FACILITY$_{(CS)}$ assumes that the enclave environment is protected from outsiders and A.DEDICATED$_{(CS)}$ assumes that the CS partition is isolated from non-administrative users within the enclave. In particular, this implies that all users that are authorized to be within the enclave but not authorized to access the TOE are physically isolated from the TOE. The accreditation required through A.FACILITY$_{(CS)}$ may be thought of as a procedure for ensuring that the organization is capable of providing the necessary protections within its operational sites to meet the requirements of OE.PHYSICAL$_{(SYS)}$.

T.TRAFFIC Use of the TOE may transmit (via traffic analysis or covert channel analysis) sensitive information to unauthorized users.

99 Direct inspection of the information sent between the two partitions is prevented by O.NO_EAVESDROP$_{(SYS)}$ prevents additional controls are required to prevent traffic analysis attacks. Effective traffic analysis may be extremely difficult to implement within the COMM, and the authorized user may apply operational controls that would lower the potential bandwidth of successful attacks (OE.OPERATE$_{(RU)}$). However, there appears to be no practical way to completely eliminate this threat.

6.2 SECURITY OBJECTIVES COVERAGE

100 This section contains two subsections, one to address the coverage of TOE Objectives and a second to address coverage Environmental Objectives. Each subsection provides a mapping table and individual arguments for the coverage of individual Objectives.

6.2.1 TOE OBJECTIVES COVERAGE

101 Table 6.3 lists either TOE Objective that require coverage in the first column. The second column provides a cross index of Policies and/or Threats that are addressed, in part or in full, by each Objective. TOE components that cover each Objective are listed in the third column.[2] Following this table are individual arguments for the coverage of each Objective.

Table 6.3 - TOE Security Objectives Coverage

Objective	Policy/Threat	Requirements	
$O.ACCESS_{(SYS)}$	P.CONFIDENTIALITY P.ELGIBLE P.INTEGRITY T.INTRUDE	$FCS\_COP.1;C_{(CS)}$ $FCS\_COP.1;D_{(RU)}$ $FDP\_IFC.1_{(CS)}$ $FDP\_IFF.1_{(CS)}$ $FDP\_ITT.2_{(SYS)}$ $FIA\_ATD.1_{(SYS)}$	$FCS\_COP.1;C_{(RU)}$ $FDP\_RIP.2_{(SYS)}$ $FDP\_IFC.1_{(SYS)}$ $FDP\_IFF.1_{(SYS)}$ $FDP\_ITT.3_{(SYS)}$
$O.AUDIT_{(SYS)}$	P.ACCOUNT	$FAU\_GEN.1_{(CS)}$ $FAU\_STG.1_{(CS)}$ $FIA\_UAU.2_{(SYS)}$ $FIA\_USB.1_{(SYS)}$	$FAU\_GEN.2_{(CS)}$ $FAU\_STG.4_{(CS)}$ $FIA\_UID.2_{(SYS)}$ $FPT\_STM.1_{(CS)}$
$O.BANNER_{(SYS)}$	P.ACCOUNT	$FTA\_TAB.1_{(SYS)}$	$FMT\_MOF.1_{(SYS)}$
$O.DETECT_{(RU)}$	P.INTEGRITY T.ALTER T.ERROR T.IMPORT T.INTRUDE T.PHYSICAL	$FAU\_ARP.1_{(RU)}$ $FCS\_COP.1;D_{(RU)}$	$FAU\_SAA.3_{(RU)}$

2. For brevity, some dependencies of the primary “covering” CC components may not be listed. However, these dependencies were considered in formation of the coverage arguments.

Table 6.3 - TOE Security Objectives Coverage

Objective	Policy/Threat	Requirements	
O.IDENTIFY$_{(SYS)}$	P.ACCOUNT P.CONFIDENTIALITY P.INTEGRITY T.INTRUDE T.MASQUERADE T.PHYSICAL	FIA_AFL1$_{(CS)}$ FIA_UAU.2$_{(SYS)}$ FIA_UAU.7$_{(SYS)}$	FIA_AFL.1$_{(RU)}$ FIA_UAU.3$_{(SYS)}$ FIA_UID.2$_{(SYS)}$
O.MANAGE$_{(SYS)}$	P.MANAGE	FMT_MOF.1$_{(SYS)}$ FMT_MSA.2$_{(SYS)}$ FMT_MTD.1$_{(SYS)}$ FMT_SAE.1$_{(CS)}$	FMT_MSA.1$_{(SYS)}$ FMT_MSA.3$_{(SYS)}$ FMT_REV.1$_{(SYS)}$ FMT_SMR.1$_{(SYS)}$
O.MEDIA$_{(RU)}$	P.CONFIDENTIALITY P.ELGIBLE P.EXPORT T.ERROR T.INTRUDE	FCS_COP.1;D$_{(RU)}$ FIA_UAU.6$_{(RU)}$	FPT_FLS.1$_{(RU)}$ FTA_SSL.1$_{(RU)}$
O.NO_EAVESDROP$_{(SYS)}$	P.CONFIDENTIALITY P.ELGIBLE P.EXPORT T.CAPTURE T.TRAFFIC	FCS_COP.1;C$_{(CS)}$ FDP_ITT.2$_{(SYS)}$ FCS_CKM.1;C$_{(SYS)}$ FCS_CKM.4$_{(SYS)}$	FCS_COP.1;C$_{(RU)}$ FCS_CKM.2;C$_{(SYS)}$ FMT_MSA.2$_{(SYS)}$
O.RECEIVE$_{(SYS)}$	P.CONFIDENTIALITY P.ELGIBLE P.EXPORT P.INTEGRITY T.CAPTURE T.ERROR	FCS_COP.1;A$_{(CS)}$ FDP_IFC.1$_{(SYS)}$ FDP_ITT.3$_{(SYS)}$	FCS_COP.1;A$_{(RU)}$ FDP_IFF.1$_{(SYS)}$ FIA_UAU.2$_{(SYS)}$
O.SELF-PROTECT$_{(SYS)}$	T.CAPTURE T.CRASH T.IMPORT	FPT_FLS.1$_{(CS)}$ FPT_ITT.2$_{(SYS)}$ FPT_RPL.1$_{(SYS)}$ FPT_SEP.1$_{(SYS)}$	FPT_FLS.1$_{(RU)}$ FPT_ITT.3$_{(SYS)}$ FPT_RVM.1$_{(SYS)}$

O.ACCESS$_{(SYS)}$ The TOE will control access to information that is subject to the enclave security policy, based on the identity of the accountable individuals, such that this policy cannot be bypassed in the TOE.

102 Users can access data controlled by the TOE either through the enclave or through a remote unit. The enclave will only deliver data to an enclave session on the CS if its security policy allows reading by the accountable individual for that session. The CS will only allow this data to flow to the RU connection associated with that session (FDP_IFC.1$_{(CS)}$ and FDP_IFF.1$_{(CS)}$). The data sent by the CS across the COMM will only be readable by the corresponding RU (FCS_COP.1;C$_{(CS)}$), being used by the same accountable individual as is associated with the enclave session. Since the user of the RU was authorized to read the data, the RU only must protect that data when the user is not present (FCS_COP.1;C$_{(RU)}$). Data and commands sent from a RU to the CS are identified with the user of the RU (FCS_COP.1;C$_{(RU)}$). Data and commands cannot be modified while in the COMM (FDP_ITT.3$_{(SYS)}$). Data and commands will be kept separate from all other information received by the CS from remote sources (FDP_IFC.1$_{(SYS)}$, FDP_IFF.1$_{(SYS)}$, and FDP_ITT.2$_{(SYS)}$). The CS will only allow this information to flow to the enclave session associated with the remote connection (FDP_IFC.1$_{(CS)}$, FDP_IFF.1$_{(CS)}$, and FIA_ATD.1$_{(SYS)}$). The enclave will treat these commands and data according to its security policy. Residual information protection (FDP_RIP.2$_{(SYS)}$) guarantees that resources allocated to one subject will not contain information from a previous subject.

O.AUDIT$_{(SYS)}$ The TOE will provide support for an audit trail to ensure each authenticated user and TOE administrator can be held accountable for his or her actions in the TOE. The audit trail will be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.

103 The minimum level of auditing was chosen for this PP because there is support within the TOE environment for some auditing functions (see OE.AUDIT). This level of auditing is sufficient because there are no untrusted users on the CS, the remote access application represents a narrow range of functionality, and the CS is dedicated to this application (see A.DEDICATED$_{(CS)}$). In addition, three components (FIA_UAU.2$_{(SYS)}$, FIA_UID.2$_{(SYS)}$, and FIA_USB.1$_{(SYS)}$) audit events at a level higher than minimum. This is a reflection of the increased importance of user I&A and accountability in a remote access application.

104 User identity is established by the TOE with identification and authentication functions (FIA_UID.2$_{(SYS)}$ and FIA_UAU.2$_{(SYS)}$). User actions are associated with system processes through the inclusion of FIA_USB.1$_{(SYS)}$ and FAU_GEN.2$_{(CS)}$.

105 The primary mechanism to record events is FAU_GEN.1$_{(CS)}$, which also specifies the details that are common to all audited events. In determining the events for which to require auditing, it is important to consider that the CS is not a general-purpose host (see A.DEDICATED$_{(CS)}$). Therefore, many events that are intended to record the activities of local, authorized users are simply not applicable. Rather than performing comprehensive auditing, only certain types of events are of interest for this TOE, specifically. The first are those events that are relevant to either the establishment of

communication between a RU and the CS. The second are other events associated with potential intrusion attempts. Because it is the enclave that must be protected from intrusions, the auditing mechanism is primarily CS-centric.

106 FPT_STM.$1_{(CS)}$ provides the capability to order events chronologically, which is crucial for the reconstruction of events. Chronological ordering also allows for the abstraction of events at a higher level of abstraction than what is actually captured by the individual audit records.

107 FAU_STG.$1_{(CS)}$ provides for the storage and protection of audit records. FAU_STG.$4_{(CS)}$ allows for two acceptable implementations for handling the case where the audit trail becomes full. In the first, additional auditable events are prevented, so the TOE "fails secure." In the second, a circular overwrite of audit trail storage is allowed. The second implementation has the advantage of allowing the TOE to remain fully functional, even in the presence of denial-of-service attacks against the CS. The possibility that audit records could be overwritten is partially offset by the relative low cost of providing a large amount of secondary storage dedicated to the audit trail. In addition, administrators in the enclave should be present and capable of reacting quickly to audit storage exhaustion, should they wish to archive the existing audit trail.

O.BANNER$_{(SYS)}$ The TOE will provide a banner to notify all users that they are entering a government computer system.

108 FTA_TAB.$1_{(SYS)}$ provides the capability to display warning banners to both authorized users logging onto the RU and administrators logging onto the CS. FMT_MOF.$1_{(SYS)}$ provides the capability for administrators to change or replace the text of the banner, as necessary.

O.DETECT$_{(RU)}$ The RU will detect unauthorized changes to its configuration.

109 The RU will detect unauthorized changes to its configuration in order to ensure an appropriate configuration and secure operation of the RU. FCS_COP.1;$D_{(RU)}$ is used to provide hashes of all security-relevant configuration data (e.g., BIOS data). These hashes are used by the FAU_SAA.$3_{(RU)}$ mechanism, which also must use the cryptographic mechanism, to determine whether this configuration data has changed while the RU is in the field. If an unauthorized change is detected, the FAU_ARP.$1_{(RU)}$ mechanism alerts the user that the configuration of the RU has been compromised.

O.IDENTIFY$_{(SYS)}$ The TOE will uniquely identify and authenticate individuals.

110 The TOE requires each user to identify itself before allowing any other TSF-mediated actions on behalf of that user, i.e. FIA_UID.$2_{(SYS)}$, and it also requires that each user be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user, FIA_UAU.$2_{(SYS)}$.

111 FIA_UAU.$3_{(SYS)}$, provides further support for this objective by preventing the forging of a users authentication data at a remote unit. An analogous requirement for

the unforgeability at the CS is considered to be desirable, but is not supported by an explicit requirement This provides the latitude for a CS to be administered from within the protected enclave with authentication data that is protected the same manner as other communications components of the protected enclave. In particular, the vulnerabilities using more forgeable authentication data, such as passwords, within the protected enclave may be balanced by the assumption that there is a reduced risk of potential exploitation.

112 The protection of authentication feedback, FIA_UAU.7$_{(SYS)}$, and the handling of authentication failures, i.e. FIA_AFL1$_{(CS)}$ and FIA_AFL.1$_{(RU)}$, provide additional support for O.IDENTIFY by reducing the opportunity for another individual to guess or derive from partial information a users authentication data.

O.MANAGE$_{(SYS)}$ The TOE will provide adequate management features for its security functions.

113 For most of the FMT (Security Management) functions, the requirements apply to the "System" partition. There are no legitimate security management activities while the RU is in the field. When FMT requirements apply to the RU, the RU is assumed to be within a secure enclave and being administered by the same administrator(s) as the CS partition.

114 With this interpretation and assumption, the security management functions and constraints are symmetrical across the partitions. Even though the system is physically distributed in its operational state, administrative functions only take place in a known environment. One FMT function (FMT_SAE.1, Time-limited authorization) applies only to the CS environment. However, the effect of this function would apply to a session establishment between a RU and the CS, and so this exception does not destroy the symmetrical property of security management functions.

115 The FMT_SMR.1$_{(SYS)}$ component allows specific individuals to be assigned the role of administrator, so that security management functions are distinct and controllable by the TOE. The role of authorized user is identified so that the set of individuals allowed to perform remote access is defined. Note that the role of administrator does not imply authorization to perform remote access. This component depends upon identification of users (FIA_UID.2$_{(SYS)}$).

116 The FMT_MSA.1$_{(SYS)}$, FMT_MSA.2$_{(SYS)}$, and FMT_MSA.3$_{(SYS)}$ components provide controls for the management of security attributes. FMT_MSA.1$_{(SYS)}$ defines the security attributes of user identity and session identifier and restricts the ability to manage these attributes to system administrators. Users are therefore not able to affect the attributes that the P.SEPARATE and P.RECEIVE policies rely upon. The FMT_MSA.2$_{(SYS)}$ component ensures that user identities, when based on cryptographic certificates, use secure values in relation to the cryptographic algorithms implemented by the TOE. Session identifier attributes may be trivially secure. Both FMT_MSA.1$_{(SYS)}$ and FMT_MSA.2$_{(SYS)}$ depend upon system security

policy definitions (FDP_IFC.$1_{(CS)}$ and FDP_IFC.$1_{(SYS)}$). In addition, FMT_MSA.$2_{(SYS)}$ depends upon a definition of secure state (and hence secure attributes), as defined in a TOE security policy model (ADV_SPM.1). FMT_MSA.$3_{(SYS)}$ provides administrators the capability to provide restrictive default values so that the default behavior of the TOE is secure with respect to the P.SEPARATE and P.RECEIVE policies.

117 The FMT_MTD.$1_{(SYS)}$ component allows administrators of the system to specify TSF data that defines the use of the TOE in its operational environment. This includes generic management functions for defining valid user identities and allowable connections between RUs and the CS. These values can only be defined in the context of the TOE's operational environment. For instance, RU peripheral devices may be authorized or not, depending upon a determination of mission needs with consideration of risk exposure.

118 The FMT_MOF.$1_{(SYS)}$ component further defines the controls for security functions of the TOE that are to be available for administrators. The administrative controls specified in this component are appropriate for managing systems providing strong I&A and basic communications functionality, and which process classified data. This determination is made by considering guidance provided in the CC for management functions in relation to the specialized functional scope of the TOE. The guidance provided by the CC is followed with the exception of those functions that are not configurable, or are otherwise not applicable, for this PP's TOE.[3]

119 The FMT_SAE.$1_{(CS)}$ component allows administrators to specify expiration times for user identities within the system. This function limits the exposure of attacks based on circumventing controls on user identities. For instance, when user identity is based on cryptographic certificates, the certificate might have a limited valid lifetime or might somehow become invalid over time. This component depends upon reliable time stamps (FPT_STM.$1_{(CS)}$).

120 Similarly, the FMT_REV.$1_{(SYS)}$ component provides for immediate, on-demand invalidation of a user's identity. This function is used for either normal termination of a user's authorization to the TOE or when a particular user's behavior becomes suspicious to administrators. Revocation could occur while the user already has a session established. It is not clear that immediate suspension of user activity is always desirable when an identity is revoked (e.g., for normal termination of an account). However, it is reasonable to assume that trivial, manual procedures – including drastic measures such as rebooting the CS – are available to administrators that want to immediately end a user's activity with the TOE.

3. A note is made in the FMT_MOF.$1_{(SYS)}$ specification for each case where the CC guidance is not followed.

O.MEDIA$_{(RU)}$ The RU will protect data stored on the unit while it is not in use and unattended.

121 This functionality is provided through FCS_COP.1;D$_{(RU)}$ and FPT_FLS.1$_{(RU)}$. FCS_COP.1;D$_{(RU)}$ provides a function to encrypt all user data on the RU disk, while FPT_FLS.1$_{(RU)}$ provides protection (e.g., of data in RAM) in case of abnormal shutdowns of the RU. The RU session-locking feature (FIA_UAU.6$_{(RU)}$ and FTA_SSL.1$_{(RU)}$) minimizes the risk of inadvertant exposure of the data on the disk if the RU is left unattended.

O.NO_EAVESDROP$_{(SYS)}$ The TOE will prevent, with a strength appropriate for tunneling classified data across a public network, the disclosure of information during transfers between a RU and the CS.

122 FDP_ITT.2$_{(SYS)}$ requires that the TOE prevent the disclosure of information passing between the RU and CS. Furthermore, the method to be used for preventing disclosure is specified through the cryptographic system requirements for the TOE. All data transmitted over the COMM is encrypted using a cryptographic system appropriate for classified information (FCS_COP.1;C$_{(CS)}$ and FCS_COP.1;C$_{(RU)}$). These functions depend on key generation, key distribution, and key destruction (FCS_CKM.1$_{(SYS)}$, FCS_CKM.2$_{(SYS)}$, and FCS_CKM.4$_{(SYS)}$) for each communications session. Secure attributes (FMT_MSA.2$_{(SYS)}$) are a property of the algorithm that implements key generation for communication sessions.

O.RECEIVE$_{(SYS)}$ A CS or a RU will only accept remote commands and data from another CS or RU with which it is mutually authenticated.

123 By the P.RECEIVE policy, remote commands and data are only accepted by a CU from a RU, or by a RU from a CU, when the RU is registered with the CU (FDP_IFC.1$_{(SYS)}$ and FDP_IFF.1$_{(SYS)}$). No other data can be inserted during transmission (FDP_ITT.3$_{(SYS)}$). Mutual cryptographic authentication between a CU and a RU (FCS_COP.1;A$_{(CS)}$ and FCS_COP.1;A$_{(RU)}$) must occur before any data can be exchanged between them (FIA_UAU.2$_{(SYS)}$).

O.SELF-PROTECT$_{(SYS)}$ The TOE will protect its security-related functions against external interference or tampering by users, attempts by users to bypass its security functions, or interruption of operation.

124 Within the RU and the CS, the TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed (FPT_RVM.1$_{(SYS)}$). It shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects (FPT_SEP.1$_{(SYS)}$). While TSF data is in transit over the COMM, it shall be protected from modification, disclosure, or replay (FPT_ITT.2$_{(SYS)}$, FPT_ITT.3$_{(SYS)}$, and FPT_RPL.1$_{(SYS)}$). In case the RU or the CS fails or is turned off, it shall maintain security (FPT_FLS.1$_{(CS)}$ and FPT_FLS.1$_{(RU)}$); in particular, open COMM connections will be dropped, requiring reauthentication before continued data exchange.

6.2.2 ENVIRONMENTAL OBJECTIVES COVERAGE

125 Table 6.4 lists Environmental Objective that require coverage in the first column. The second column provides a cross index of Policies and/or Threats that are addressed, in part or in full, by each Objective. Environmental requirements that cover each Objective are listed in the third column.[4] Following this table are individual arguments for the coverage of each Objective.

Table 6.4 - Environmental Security Objectives Coverage

Objective	Policy/Threat	Requirements	
OE.AUDIT$_{(CS)}$	P.ACCOUNT	FAU_ARP.1$_{(ENV)}$	FAU_SAA.1$_{(ENV)}$
		FAU_SAA.1$_{(ENV)}$	FAU_SAR.1$_{(ENV)}$
		FAU_SAR.2$_{(ENV)}$	FAU_SAR.3$_{(ENV)}$
		ADMIN$_{(ENV)}$	RESPONSE$_{(ENV)}$
		REVIEW$_{(ENV)}$	
OE.CRYPTOKEYS$_{(SYS)}$	P.CONFIDENTIALITY	FCS_CKM.1$_{(ENV)}$	FCS_CKM.4$_{(ENV)}$
		FMT_MSA.2$_{(ENV)}$	
OE.OPERATE$_{(RU)}$		CONNECT$_{(ENV)}$	DUE_CARE$_{(ENV)}$
		PERIPHERALS$_{(ENV)}$	SINGLE_USER$_{(ENV)}$
		TRAINING$_{(ENV)}$	
OE.ACCREDITED$_{(SYS)}$		ACCREDIT$_{(ENV)}$	
OE.ADMIN$_{(SYS)}$		ADMIN$_{(ENV)}$	AUTHORIZED$_{(ENV)}$
		INSTALL$_{(ENV)}$	PERIPHERALS$_{(ENV)}$
		TRAINING$_{(ENV)}$	
OE.CLEARED$_{(SYS)}$	P.ELGIBLE P.EXPORT P.MARKING T.PHYSICAL	CLEARED$_{(ENV)}$	AUTHORIZED$_{(ENV)}$
OE.INSTALL$_{(SYS)}$	P.MANAGE T.IMPORT	INSTALL$_{(ENV)}$	ISOLATION$_{(ENV)}$
		TRAINING$_{(ENV)}$	EAL5

4. For brevity, some dependencies of the primary “covering” CC components may not be listed. However, these dependencies were considered in formation of the coverage arguments.

Table 6.4 - Environmental Security Objectives Coverage

Objective	Policy/Threat	Requirements
$OE.PHYSICAL_{(SYS)}$	P.ELGIBLE T.ALTER T.CAPTURE T.INTRUDE T.PHYSICAL T.TRAFFIC	$DUE\_CARE_{(ENV)}$ $PHYSICAL_{(ENV)}$
$OE.TRAINED_{(SYS)}$	P.EXPORT P.MANAGE P.MARKING T.IMPORT T.TRAFFIC	$TRAINING_{(ENV)}$

$OE.AUDIT_{(CS)}$ Enclave personnel will apply technical, procedural, and administrative controls that are sufficient to maintain user accountability throughout the enclave.

126 $ADMIN_{(ENV)}$ supports this objective by requiring the assignment of at least one person to act in the role of administrator. The administrator is expected to review the TOE audit records periodically to maintain a secure environment. Lack of review of the audit features, could inadvertently open a vulnerability in the TOE. There are procedural requirements to be responsive to security alarms ($RESPONSE_{(ENV)}$) and to conduct periodic reviews ($REVIEW_{(ENV)}$). The IT environment provides the administrator capabilities to read and interpret the audit records generated by the TOE ($FAU\_SAR.1_{(ENV)}$). The IT environment enhances these capabilities by providing searching and sorting features ($FAU\_SAR.3_{(ENV)}$). Accessing and interpreting the audit data must be restricted from other users in the enclave, who may not be authorized for such data ($FAU\_SAR.2_{(ENV)}$). Audit review capabilities complement the interpretation of intrusion scenarios that are defined for the analysis mechanism ($FAU\_SAA.1_{(ENV)}$) and the alarm mechanism ($FAU\_ARP.1_{(ENV)}$). Because intrusion is an enclave-wide threat, the problem must be addressed at that level, rather than at the level of each individual system (e.g., the remote access TOE).

$OE.CRYPTOKEYS_{(SYS)}$The Department of Defense, Public Key Infrastructure will provide the necessary key initialization to support the CS/RU authentication function and the media encryption function on the RU.

127 Both the CS/RU authentication function and the media encryption mechanism on the RU require key management functions. These key management functions include secure key generation ($FCS\_CKM.1_{(ENV)}$) and key destruction ($FCS\_CKM.4_{(ENV)}$). These functions need not be a part of the TOE, consistent with the concept of operations for an external, public-key infrastructure. $FMT\_MSA.2_{(SYS)}$ guarantees

that the attributes supported by the key management functions are adequate for the cryptographic functions they support.

OE.OPERATE$_{(RU)}$Authorized users operate the RU in a manner that maintains the system security.

128 The authorized user of the RU must be adequately trained in the secure operation of the TOE (TRAINING$_{(ENV)}$) and must follow that training. Secure operation of the RU includes the appropriate settings for its use as well as storage and protection of the RU while it is not in use (DUE_CARE$_{(ENV)}$).The RU user must not attempt to connect to arbitrary communications servers, some of which might be operated by malicious parties (CONNECT$_{(ENV)}$). The RU user must not allow unauthorized parties to use the RU after having established a connection to the CS (SINGLE_USER$_{(ENV)}$). The RU user must also not connect unauthorized peripherals to the RU, which could circumvent protection features of the TOE (PERIPHERALS$_{(ENV)}$).

OE.ACCREDITED$_{(SYS)}$The enclave will be accredited to operate the TOE.

129 The organization that operates the enclave must get formal approval to operate the TOE within the intended environment of use (ACCREDIT$_{(ENV)}$).

OE.ADMIN$_{(SYS)}$Administrators manage the remote access system in a manner that maintains the system security.

130 There must be at least one individual to fill the role of administrator (ADMIN$_{(ENV)}$). The administrator must not allow use of the TOE by unauthorized individuals (AUTHORIZED$_{(ENV)}$). The administrator must install the TOE correctly (INSTALL$_{(ENV)}$) and must never attach unauthorized devices that could compromise security (PERIPHERALS$_{(ENV)}$). The administrator must be adequately trained in the secure operation of the TOE (TRAINING$_{(ENV)}$) and must follow that training.

OE.CLEARED$_{(SYS)}$ Authorized users and administrators must receive formal clearance before they can access the TOE.

131 The organization operating the enclave must ensure that all users and administrators are cleared (CLEARED$_{(ENV)}$) and authorized (AUTHORIZED$_{(ENV)}$) for information accessible to them through the TOE. These administrative requirements constitute the intent of the term “formal clearance.”

132 The functional security mechanisms of the TOE are expected to provide the necessary mechanisms to thwart unauthorized access due to lack of appropriate clearance. Mechanisms such as FIA_ATD.1$_{(SYS)}$, FDP_ITT.2$_{(SYS)}$, FMT_MSA.1$_{(SYS)}$ and requirements supplement this environmental objective within the TOE.

OE.INSTALL$_{(SYS)}$The remote access system is delivered and installed in a manner that maintains the system security.

133 The remote access system will be delivered, installed, managed and operated in a manner which maintains the system security. EAL5 specifies the appropriate assurance requirements to ensure the TSF has met the necessary developmental, operational and maintenance aspects of the TOE. $INSTALL_{(ENV)}$ reflects the basic requirement for the enclave to conduct a secure installation procedure. As a part of this procedure, the CS must be physically isolated from non-administrative users in the enclave ($ISOLATION_{(ENV)}$).

OE.$PHYSICAL_{(SYS)}$TOE hardware, software, and documentation, and all classified data handled by the TOE are physically protected to prevent unauthorized (intentional or unintentional) disclosure.

134 It is assumed that all TOE components will be physically protected to the degree commensurate with the level of the information processed by in the TOE as provided by the requirement $PHYSICAL_{(ENV)}$. Additionally, $DUE\_CARE_{(ENV)}$ is intended to direct the users of the RU to take the necessary measures to protect the RU when outside of the enclave and while the RU is not in use.

OE.$TRAINED_{(SYS)}$Train authorized users and administrators about relevant security policies and the practices they need to follow to establish and maintain adequate security.

135 All users and administrators of the remote access system are expected to be trained in proper operation of the system. Failure to conduct proper training on the operation of the security attributes and functions of the system could result in failure of the TSF. The non-IT requirement $TRAINING_{(ENV)}$ identifies the need for an effective training plan to be established to support the proper use and operation of the remote access system.

6.3 ARGUMENT THAT EAL5 IS APPROPRIATE

136 For high-assurance TOEs, DoD policy requires an EAL "greater than EAL4" [TBD - reference the policy document that describes this & add to reference list]. EAL5 meets this criteria and provides a full measure of assurance that accompanies a CC-defined EAL.

137 For the environment described for this TOE, threat agents are sophisticated and the information protected by the TOE is very sensitive. With such an environment, it is reasonable to expect significant expense in the area of security engineering of a product. A relatively higher degree of security technology engineering is expected to be applied for a TOE in this environment. This additional expense is very likely to be more than that expected for basic commercial development practices (i.e., EAL4).

138 The TOE described in this PP is a system that could potentially (by intent) be integrated from components produced by more than one development organization. The case of independent integration is highlighted because this as a worst-case scenario when compared to a single organization building (and integrating internally) all the components of the TOE. Each individual development organization could have its own degree of capability in the area of security engineering. The integrator of such a TOE must at least be capable of a moderate application of security engineering technology in order to adequately protect sensitive assets from sophisticated threats.

139 In general, an integration scenario is compatible with EAL5 because the integration organization can be expected to have an appropriate degree of security engineering capability, or otherwise rejected in favor of one that does. Integration is compatable with heterogenous development organizations, because a knowledgeable integrator could reject components that had not been produced with adequate security engineering practices.

140 In contrast, an integration scenario limits the upper bound of assurance that might be achieved with a single development organization. EAL6 requires such a rigorous development environment that it is more suited to a single development organization. Multiple development organizations would tend to reduce the rigor, and increase the costs, of the rigorous development environment required for EAL6. Therefore, EAL6 is considered to be inappropriate for this TOE.

6.4 MINIMUM SOF ARGUMENTS

141 The strength-of-function (SoF) claim for this PP is SoF-High. This claim is based upon the fact that the TOE will process classified information related to national security. The application (remote access) and the distributed nature of TOE components imply that threat agents could have complete access to the TOE for an extended period of elapsed time. Furthermore, threat agents are likely to be state-sponsored, and therefore are potentially experts with extensive knowledge of the TOE, and would have the means to produce commissioned tools.

142 The TOE objectives of this PP must enforce TOE policies and counter TOE-relevant threats with a degree of effectiveness that is commensurate with the threat posed. The

risk environment is comprised of a very sophisticated threat agent in conjunction with very sensitive data. Thus, a rating of SoF-High is consistent with the TOE objectives included in this PP

6.5 DEPENDENCY RATIONALE

143 This section provides the dependency analyses for functional and assurance requirements, and rationale for missing dependencies. For the purposes of dependency analysis, the scope of the dependent component must be less than or equal to that of each component used to satisfy the dependencies.

6.5.1 FUNCTIONAL REQUIREMENTS DEPENDENCY ANALYSIS

144 Table 6.5 contains the dependency analysis for the functional components. The first column provides a reference number. The second column provides the component identifier. The third column provides dependencies for that component. The last column provides a cross reference to the component that satisfies the dependency. Unless otherwise noted, all cross-references in the fourth column pertain to Table 6.5 Finally, the fifth column shows that the scope of the dependent component is less than or equal to that of the dependent.[1]

145

Table 6.5 - Functional Requirements Dependencies

Index	Requirement	Dependencies	Coverage	Scope Analysis
1	FAU_ARP.1$_{(RU)}$	FAU_SAA.1	4	RU = RU
2	FAU_GEN.1$_{(CS)}$	FPT_STM.1	46	CS = CS
3	FAU_GEN.2$_{(CS)}$	FAU_GEN.1 FIA_UID.1	2 29	CS = CS CS < SYS
4	FAU_SAA.3$_{(RU)}$	none	N/A	
5	FAU_STG.1$_{(CS)}$	FAU_GEN.1	2	CS = CS
6	FAU_STG.4$_{(CS)}$	FAU_STG.1	5	CS = CS
7	FCS_CKM.1$_{(SYS)}$	FCS_COP.1 FCS_CKM.4 FMT_MSA.2	12 and 13 9 33	SYS = CS + RU SYS = SYS SYS = SYS
8	FCS_CKM.2$_{(SYS)}$	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	7 9 33	SYS = SYS SYS = SYS SYS = SYS
9	FCS_CKM.4$_{(SYS)}$	FCS_CKM.1 FMT_MSA.2	7 33	SYS = SYS SYS = SYS
10	FCS_COP.1;A$_{(CS)}$	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	See Section 6.5.3.	

1. All assurance components are considered to have a SYS scope. Also, a combined scope of CS + RU is considered equivalent to a scope of SYS.

Table 6.5 - Functional Requirements Dependencies

Index	Requirement	Dependencies	Coverage	Scope Analysis
11	FCS_COP.1;$A_{(RU)}$	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	See Section 6.5.3.	
12	FCS_COP.1;$C_{(CS)}$	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	7 9 33	CS < SYS CS < SYS CS < SYS
13	FCS_COP.1;$C_{(RU)}$	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	7 9 33	RU < SYS RU < SYS RU < SYS
14	FCS_COP.1;$D_{(RU)}$	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	See Section 6.5.3.	
15	FDP_IFC.$1_{(CS)}$	FDP_IFF.1	17	CS = CS
16	FDP_IFC.$1_{(SYS)}$	FDP_IFF.1	19	SYS = SYS
17	FDP_IFF.$1_{(CS)}$	FDP_IFC.1 FMT_MSA.3	15 34	CS = CS CS < SYS
18	FDP_IFF.$1_{(SYS)}$	FDP_IFC.1 FMT_MSA.3	16 34	SYS = SYS SYS = SYS
19	FDP_ITT.$2_{(SYS)}$	FDP_IFC.1	16	SYS = SYS
20	FDP_ITT.$3_{(SYS)}$	FDP_IFC.1 FDP_ITT.1	16 19	SYS = SYS SYS = SYS
21	FDP_RIP.$2_{(RU)}$	none	N/A	
22	FIA_AFL.$1_{(CS)}$	FIA_UAU.1	25	CS < SYS
23	FIA_AFL.$1_{(RU)}$	FIA_UAU.1	25	RU < SYS
24	FIA_ATD.$1_{(SYS)}$	none	N/A	
25	FIA_UAU.$2_{(SYS)}$	FIA_UID.1	29	SYS = SYS
26	FIA_UAU.$3_{(SYS)}$	none	N/A	
27	FIA_UAU.$6_{(RU)}$	none	N/A	
28	FIA_UAU.$7_{(SYS)}$	FIA_UAU.1	25	SYS = SYS
29	FIA_UID.$2_{(SYS)}$	none	N/A	
30	FIA_USB.$1_{(CS)}$	FIA_ATD.1	24	CS < SYS
31	FMT_MOF.$1_{(SYS)}$	FMT_SMR.1	38	SYS = SYS

Table 6.5 - Functional Requirements Dependencies

Index	Requirement	Dependencies	Coverage	Scope Analysis
32	FMT_MSA.1$_{(SYS)}$	FDP_IFC.1 FMT_SMR.1	15 and 16 38	SYS = SYS SYS = SYS
33	FMT_MSA.2$_{(SYS)}$	ADV_SPM.1 FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	61 (Table 6.6) 15 and 16 32 38	SYS = SYS SYS <= SYS + CS SYS = SYS SYS = SYS
34	FMT_MSA.3$_{(SYS)}$	FMT_MSA.1 FMT_SMR.1	32 38	SYS = SYS SYS = SYS
35	FMT_MTD.1$_{(SYS)}$	FMT_SMR.1	38	SYS = SYS
36	FMT_REV.1$_{(SYS)}$	FMT_SMR.1	38	SYS = SYS
37	FMT_SAE.1$_{(CS)}$	FMT_SMR.1 FPT_STM.1	38 46	CS < SYS CS = CS
38	FMT_SMR.1$_{(SYS)}$	FIA_UID.1	29	SYS = SYS
39	FPT_FLS.1$_{(CS)}$	ADV_SPM.1	61 (Table 6.6)	CS < SYS
40	FPT_FLS.1$_{(RU)}$	ADV_SPM.1	61 (Table 6.6)	CS < SYS
41	FPT_ITT.2$_{(SYS)}$	none	N/A	
42	FPT_ITT.3$_{(SYS)}$	FPT_ITT.1	41	SYS = SYS
43	FPT_RPL.1$_{(SYS)}$	none	N/A	
44	FPT_RVM.1$_{(SYS)}$	none	N/A	
45	FPT_SEP.1$_{(SYS)}$	none	N/A	
46	FPT_STM.1$_{(CS)}$	none	N/A	
47	FPT_TDC.1$_{(SYS)}$	none	N/A	
48	FTA_SSL.1$_{(RU)}$	FIA_UAU.1	25	RU < SYS
49	FTA_TAB.1$_{(SYS)}$	none	N/A	

146

6.5.2 Assurance Requirements Dependency Analysis

147 Table 6.6 contains the dependency analysis for the assurance components. The first column provides a reference number. The second column provides the component identifier. The third column provides dependencies for that component. The last column provides a cross reference to the component that satisfies the dependency. All

cross-references in the fourth column pertain to Table 6.6. Because the scope of all assurance requirements is equivalent to SYS, no scope analysis is necessary.

Table 6.6 - Assurance Requirements Dependencies

Index	Requirement	Dependencies	Coverage
50	ACM_AUT.1	ACM_CAP.3	51
51	ACM_CAP.4	ACM_SCP.1 ALC_DVS.1	52 64
52	ACM_SCP.3	ACM_CAP.3	51
53	ADO_DEL.2	ACM_CAP.3	51
54	ADO_IGS.1	AGD_ADM.1	62
55	ADV_FSP.3	ADV_RCR.1	60
56	ADV_HLD.3	ADV_FSP.3 ADV_RCR.2	55 60
57	ADV_IMP.2	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	59 60 66
58	ADV_INT.1	ADV_IMP.1 ADV_LLD.1	57 59
59	ADV_LLD.1	ADV_HLD.2 ADV_RCR.1	56 60
60	ADV_RCR.2	none	N/A
61	ADV_SPM.3	ADV_FSP.1	55
62	AGD_ADM.1	ADV_FSP.1	55
63	AGD_USR.1	ADV_FSP.1	55
64	ALC_DVS.1	none	N/A
65	ALC_LCD.2	none	N/A
66	ALC_TAT.2	ADV_IMP.1	57
67	ATE_COV.2	ADV_FSP.1 ATE_FUN.1	55 69
68	ATE_DPT.2	ADV_HLD.2 ADV_LLD.1 ATE_FUN.1	56 59 69
69	ATE_FUN.1	none	N/A
70	ATE_IND.2	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	55 62 63 69

Table 6.6 - Assurance Requirements Dependencies

Index	Requirement	Dependencies	Coverage
71	AVA_CCA.1	ADV_FSP.2 ADV_IMP.2 AGD_ADM.1 AGD_USR.1	55 57 62 63
72	AVA_MSU.2	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	54 55 62 63
73	AVA_SOF.1	ADV_FSP.1 ADV_HLD.1	55 56
74	AVA_VLA.3	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1	55 56 57 59 62 63

148

6.5.3 Rationale for Allocating Some Dependencies to the Environment[2]

149 Three components in this PP have their dependencies satisfied by the following three, environmental components: FCS_CKM.1$_{(ENV)}$, FCS_CKM.4$_{(ENV)}$, and FMT_MSA.2$_{(ENV)}$. These environmental components correspond to external key management functions that would be typical of a DoD public-key infrastructure. This PP anticipates the establishment of that infrastructure for the RU's media encryption function (FCS_COP.1;D$_{(RU)}$) and the CS/RU mutual authentication function (FCS_COP.1;A$_{(CS)}$ and FCS_COP.1;A$_{(RU)}$). Note that the public-key infrastructure does not need to be established for the entire DoD; any organization that fields the TOE could establish a local public-key infrastructure. Any such infrastructure would be capable of serving multiple applications, and therefore is better served by an independent specification of its requirements. Any infrastructure provided by the environment must satisfy the dependencies the TOE has for the functions listed above. However, these dependencies are typical of state-of-the-practice public-key infrastructures, and therefore do not represent an extreme or unreasonable burden on the fielding organization.

150 For both the RU media encryption function and the CS/RU mutual authentication function, having the key management functional dependencies satisfied by an external (i.e., non-TOE) entity provides some beneficial risk trade-offs. When allocated to an external entity, an attack that successfully circumvents the TOE cannot, by itself, also undermine the key management support. This not only protects

2. This section substitutes for "Rationale for not satisfying all dependencies." Besides those dependencies that are satisfied by the TOE Environment, all other dependencies in this PP are satisfied by the TOE.

data on a specific RU or during a specific session, but also other RUs or CSs that use the same public key infrastructure. The allocation of the dependencies for these functions to the environment also have the positive side effect of simplifying and minimizing the functions of the TOE, which must be implemented with high assurance.

6.6 MUTUALLY SUPPORTIVE AND INTERNALLY CONSISTENT ARGUMENTS

151 This section provides arguments that the TOE requirements form a mutually supportive and internally consistent whole.

6.6.1 OVERVIEW

152 The system has a natural decomposition into three logical components.[1] This decomposition reflects the fact that there are three distinctly different sub-environments that are part of the system environment: the environment local to a traveling users, the COMM environment, and the environment local to the enclave. The effectiveness of the security functional requirements at mitigating the risks from specific threats have a similar decomposition associated with those three sub-environments. As a result, some of the functional security requirements of the TOE are only needed for a specific sub-environment. For the convenience of specifying those requirements that need only apply to a portion of the TOE, two distinct TOE partitions are identified: a Remote Unit (RU) partition and a Communications Server (CS) partition. A RU contains those parts of the system that a user takes to a remote location, while the CS is the part of the system that remains within the security perimeter of the enclave and connects the enclave with the COMM. The system (SYS) partition is used to denote a functional obligation for both the RU and CS partitions. This section provides further rationale for the chosen approach and the associated decision not to include a separate partition for the COMM.

153 The interfaces to the system have been selected to be the user interfaces to the RU (e.g. the keyboard, mouse, display, and token interfaces, the interface between the RU and the COMM, the interface between the COMM and the CS, the interface of the CS to the backbone network of the enclave, and (possibly) a direct administrative console interface to the CS. Based upon the three distinct threat environments, the system splits into three partitions: the RU, the CS, and the COMM. A decision was made to place all the hardware and/or software required to encrypt/decrypt communications within the RU or the CS components. An alternative would have been to incorporate the encryption/decryption hardware and software within the COMM component. This would have amounted to splitting the Remote Unit into a Remote Unit Workstation and a Remote Encryption Unit/Modem and similarly splitting off the encryption/modem unit from the communications server. This would have the advantage of making it easier to specify distinct assurance requirements for the encryption/modem units. The following factors were taken into consideration in deciding not to take that alternative approach:

a) There are reasons for placing comparable assurance requirements on other aspects of the Remote Unit and the interface between the encrypting modem and the Communications Server. At the chosen assurance level, the decomposition into a modules that perform the COMM encryption/decryption and the demonstration of the non-bypassability of those modules are part of

1. The TOE environment (i.e., the ENV partition) is not part of the decomposition of the system. The concept of the TOE environment uses some of the naming conventions of the system partitions because it is a convenient abstraction for describing the scope of requirements.

the system architecture requirements specified by the assurance requirements. By not explicitly calling out a separate hardware unit, the system developer is given the same option to build the remote unit out of separate hardware components while also giving the developer the flexibility to incorporate functionality into a single hardware unit with the equivalent internal design constraints.

b) The adversaries are assumed to have direct access to the underlying COMM communications. As a result, the security properties of the interface between the modem and the encryption unit would still need to be specified at an equivalent level of detail as that required in the current architecture.

c) It is believed that there are possible solutions utilizing encrypting modems that are capable of synchronizing with and establishing encrypted sessions with other encrypting modems. For example, two separate copies of the same remote access solution might result in the modem from the RU for one system being able to connect with the modem from the other systems CS. The requirements for communication between TOE partitions that have been defined in the present profile address this concern, but they would not have been sufficient if the COMM was itself a partition. Additional requirements for the passing of authentication information would have to be made about the interfaces between the remote encrypting modems and the remote unit workstation and also about the encrypting modems interface with the CS.

d) The previous consideration highlights another technical concern that the profile writers tried to address. Namely, the question of when the TOE was in an evaluated mode of operation. Trusted systems have typically had some form of initialization process during which the TOE is not in secure state. Distributed systems have always provided an extra nuance to the concept of secure state, because each distributed component may operate independently in a secure state and there needs to be a means for the distributed components of a TOE to join in communications while components are already operating in secure state. The chosen profile allows the TOE to be in secure state when the RU is being used locally and is not connected to the CS. Placing the encrypting modems within the COMM partition, would have unnecessarily recreated the problem of defining and establishing a distributed secure state within a single partition.

6.6.2 SEMANTICS OF COVERAGE ANALYSIS

154 This PP addresses a security problem that is stated in terms of Policies to be supported and Threats to be countered. For semantic coherency, the PP does not divide this problem in terms of environment partitions, precisely because the security problem must be addressed uniformly across all environmental partitions. All other constructs (e.g., assumptions, components, and environmental requirements) of the PP have an environmental context or scope, and the specific identifier subscript (i.e., CS, RU, SYS, COMM, or ENV) reflects that context. The SYS qualifier has special semantics, in that it means the PP construct has equal relevance for all partitions—it can be thought of as the logical "AND" of the CS and RU context.[2]

155 The Policies and Threats coverage provided in this PP must take into account partition constraints. CS constructs are not applicable in the RU environment, and RU constructs are not applicable in the CS environment. In contrast, SYS constructs are applicable in both CS and RU environments. As mentioned above, both partition environments must provide uniform coverage of each Policy and Threat in the PP. Semantic coherency is maintained in this PP by using only valid combinations of constructs to provide coverage arguments. This methodology is described abstractly in the following series of figures. Note that the associations provided in the figures do not relate to "sufficiency" or "necessity" aspects of coverage. Rather, the associations provided in the figures relate to the bounds from which constructs can be used

156

$$A \in \{Assumptions\}$$

$$coverage(A) \Leftarrow \{EnvironmentalObjectives\}$$

Figure 1. Semantic coherency of assumption coverage analysis

157 Figure 2 shows that the analysis of objective coverage for each Policy and Threat is determined by assessing whether each Policy and Threat is adequately addressed within both partitions.[3] Objective coverage analysis is performed by examining each partition individually. The objectives relevant to the CS partition are those with either the CS or SYS scope (i.e., a logical OR relationship). Similarly, the objectives relevant to the RU partition are those with either the RU or SYS scope. Finally, the coverage of each partition must be done independent of the other (i.e., a logical AND relationship), because each Policy and Threat must be fully covered in both partitions.

158

$$S \in \{Policy\} \cup \{Threats\}$$

$$coverage(S) \Leftarrow objectives(CS \vee SYS) \wedge objectives(RU \vee SYS)$$

Figure 2. Semantic coherency of objective coverage analysis

2. The Policies and Threats expressed in this PP might reasonably be considered as having a "SYS" context.
3. For simplification, Assumptions are factored out of this figure. Also, note that it is not relevant to the assessment of coverage whether Objectives are assigned to the TOE or to the environment.

159 Figure 3 shows the method of requirements-coverage analysis for TOE Objectives.[4] There are three relevant cases for performing this analysis. Objectives having a CS-only scope can be covered by components having either a CS or SYS scope. Objectives having a RU-only scope can be covered by components having either a RU or SYS scope. Finally, Objectives having a SYS scope must be independently covered within both the CS scope and the RU scope.

160 The objectives relevant to the CS partition are those with either the CS or SYS scope (i.e., a logical OR relationship). Similarly, the objectives relevant to the RU partition are those with either the RU or SYS scope. Finally, the coverage of each partition must be done independent of the other (i.e., a logical AND relationship), because each Policy and Threat must be fully covered in both partitions.

161

$$coverage[Objective(CS)] \Leftarrow components(CS \vee SYS)$$

$$coverage[Objective(RU)] \Leftarrow components(RU \vee SYS)$$

$$coverage[Objective(SYS)] \Leftarrow components(CS \vee SYS) \wedge components(RU \vee SYS)$$

Figure 3. Semantic coherency of TOE requirements coverage analysis

162 This PP is semantically coherent in that the assumption, objective, and requirement coverage arguments (represented by Tables 6.1, 6.2, and 6.3, respectively) all follow the constraints of these relations. Note that this PP defines a very simple partitioning of the system, and does not present a generalized approach. We assume that a generalized approach would be compatible, although possibly much more complex.

6.6.3 IDENTIFICATION OF TOE REQUIREMENTS

163 Each of the TOE security functional requirements (SFRs) used in this PP (see 5.2) use components defined in Part 2 of the CC. The identifiers for these SFRs are based on the CC identifiers, using subscripts to identify specific system partitions where the SFR is implemented. The SYS subscript is used consistently, signifying that an SFR must be implemented on both partitions. When a CC component is iterated within the same partition, a unique suffix is appended to distinguish the iterations.

164 Operations carried out on each CC-derived component follow CC guidance for the specification of assignments, selections, refinements, and iterations. The conventions

4. Note that requirements coverage analysis is not required by the CC for environmental objectives. Also note that there are no TOE objectives levied on the COMM partition.

used to identify these operations in the text of the SFRs is explained under the heading "Conventions" on page v.

165 This PP specifies a CC-defined assurance package (EAL4 ++) for the TOE. The identification of these requirements exactly follows that used by the CC. The specification of non-TOE IT requirements are based on CC conventions with unique identification conventions applied, and non-TOE environmental requirements follows an unambiguous and consistent naming convention.

6.6.4 COMPATIBLE FUNCTIONALITY OF THE SFRS

166 Non-bypassability of the TSP is required (FPT_RVM.$1_{(SYS)}$). The PP specifies functions that prevent the bypassing of many of the TOE SFRs. (For instance, the TOE protects theft of TSF data (e.g., key values) that protect the confidentiality of user data (FPT_ITT.$2_{(SYS)}$). If one of the partitions fails, it fails with the preservation of a secure state (FPT_FLS.$1_{(CS)}$ and FPT_FLS.$1_{(RU)}$). Residual information protection (FDP_RIP.$2_{(RU)}$) prevents circumvention of user data confidentiality on the RU if the unit is stolen. Security alarms (FAU_ARP.$1_{(CS)}$ and FAU_ARP.$1_{(RU)}$) protect against prolonged attacks on the I&A mechanism.

167 TOE user access controls defined for this PP (see FDP_IFC and FDP_IFF components) are supported through the inclusion of requirements for user I&A (FIA_UID.2(SYS) and FIA_UAU.2(SYS)). Circumvention of user I&A is protected against through the inclusion of three sets of requirements: authentication failure handling (FIA_AFL.$1_{(CS)}$ and FIA_AFL.$1_{(RU)}$), unforgeable authentication data on the RU (FIA_UAU.$1_{(RU)}$), and protected authentication data feedback (FIA_UAU.$7_{(SYS)}$).

168 The TOE is self-protecting in it's inclusion of TSF domain separation (FPT_SEP.$1_{(SYS)}$). The TOE also protects itself from tampering attacks against sensitive TSF data (e.g., key values), while it traverses the COMM (FPT_ITT.$3_{(SYS)}$). The TOE provides secure time stamps (FPT_STM.$1_{(CS)}$), and the audit trail is protected (FAU_STG.$1_{(CS)}$ and FAU_STG.$4_{(CS)}$), so that the audit trail accurately represents user activity on the system. Security attributes and other TSF data are protected from unauthorized tampering by the inclusion of appropriate administrative management (FMT_MSA.$1_{(SYS)}$ and FMT_MSA.$3_{(SYS)}$).

169 The assurance requirements of EAL5 provide confidence that the functional requirements are met, and so by definition these requirements support the compatible functionality of the SFRs.

6.6.5 TOE ASSUMPTIONS COHERENCY

170 The environmental assumptions made in this TOE are all based on common security practices and expectations. These assumptions reflect common characteristics of many current security environments.

171 A.CONTROLLED$_{(RU)}$ and A.DEDICATED$_{(CS)}$ are easily converted into operational requirements that can be clearly understood, can be implemented without

extreme difficulty, and do not place an unreasonable operating burden on the organization.

172 $A.FACILITY_{(CS)}$ is a common property of DoD enclaves, and translates to requirements that are often implemented without regard to the specific requirements of the PP or to remote access in general. This assumption adds no new degree of difficulty to this commonly existing practice.

173 $A.TRUSTED\_ADMIN_{(SYS)}$ and $A.TRUSTED\_USER_{(SYS)}$ are common and reasonable assumptions that convert to a well-understood set of administrative requirements, procedures for deterrence, and knowledge of expected behavior.

6.7 NECESSITY ARGUMENTS

174 This section provides tables showing that all components and objectives used in this PP are necessary. The following subsections provide individual arguments:

175 Section 6.6.1 shows that each environmental component is mapped to at least one environmental objective.

176 Section 6.6.2 shows that each TOE component is mapped to at least one TOE objective.

177 Section 6.6.3 shows that each environmental objective is mapped to at least one policy or threat.

178 Section 6.6.4 shows that each TOE objective is mapped to at least one policy or threat.

179 Because of the structure of these arguments, we can conclude that each component included in PP is necessary to support

6.7.1 NECESSITY ARGUMENT FOR ENVIRONMENTAL COMPONENTS

180 The following table shows that each environmental component is mapped to at least one environmental objective.

Table 6.7 - Necessity of Environmental Requirements

Component	OE.AUDIT$_{(CS)}$	OE.CRYPTOKEYS$_{(SYS)}$	OE.OPERATE$_{(RU)}$	OE.ACCREDITED$_{(SYS)}$	OE.ADMIN$_{(SYS)}$	OE.CLEARED$_{(SYS)}$	OE.INSTALL$_{(SYS)}$	OE.PHYSICAL$_{(SYS)}$	OE.TRAINED$_{(SYS)}$
FAU_SAR.1$_{(ENV)}$	X								
FAU_SAR.2$_{(ENV)}$	X								
FAU_SAR.3$_{(ENV)}$	X								
FCS_CKM.1$_{(ENV)}$		X							
FCS_CKM.4$_{(ENV)}$		X							
FMT_MSA.2$_{(ENV)}$		X							
ACCREDIT$_{(ENV)}$				X					
ADMIN$_{(ENV)}$	X				X				
AUTHORISED$_{(ENV)}$					X	X			
CLEARED$_{(ENV)}$						X			
CONNECT$_{(ENV)}$			X						
DUE_CARE$_{(ENV)}$			X					X	
INSTALL$_{(ENV)}$					X		X		
ISOLATION$_{(ENV)}$							X		
PERIPHERALS$_{(ENV)}$			X		X				
PHYSICAL$_{(ENV)}$								X	
RESPONSE$_{(ENV)}$	X								
REVIEW$_{(ENV)}$	X								
SINGLE_USER$_{(ENV)}$			X						
TRAINING$_{(ENV)}$			X		X		X		X

6.7.2 NECESSITY ARGUMENT FOR TOE COMPONENTS

181 The following table shows that each TOE functional component is mapped to at least one TOE objective.

Table 6.8 - Necessity of TOE Requirements

		O.DETECT$_{(RU)}$	O.MEDIA$_{(RU)}$	O.ACCESS$_{(SYS)}$	O.AUDIT$_{(SYS)}$	O.BANNER$_{(SYS)}$	O.IDENTIFY$_{(SYS)}$	O.MANAGE$_{(SYS)}$	O.NO_EAVESDROP$_{(SYS)}$	O.RECEIVE$_{(SYS)}$	O.SELF-PROTECT$_{(SYS)}$
1	FAU_ARP.1$_{(CS)}$				X						
2	FAU_ARP.1$_{(RU)}$	X									
3	FAU_GEN.1$_{(CS)}$				X						
4	FAU_GEN.2$_{(CS)}$				X						
5	FAU_SAA.1$_{(CS)}$				X						
6	FAU_SAA.3$_{(RU)}$	X									
7	FAU_STG.1$_{(CS)}$				X						
8	FAU_STG.4$_{(CS)}$				X						
9	FCS_CKM.1$_{(SYS)}$								X		
10	FCS_CKM.2$_{(SYS)}$								X		
11	FCS_CKM.4$_{(SYS)}$								X		
12	FCS_COP.1;C$_{(CS)}$			X					X	X	
13	FCS_COP.1;C$_{(RU)}$			X					X	X	
14	FCS_COP.1;D$_{(RU)}$	X	X	X							
15	FDP_IFC.1$_{(CS)}$			X							
16	FDP_IFC.1$_{(SYS)}$			X						X	
17	FDP_IFF.1$_{(CS)}$			X							
18	FDP_IFF.1$_{(SYS)}$			X						X	
19	FDP_ITT.2$_{(SYS)}$			X					X		
20	FDP_ITT.3$_{(SYS)}$			X						X	
21	FDP_RIP.2$_{(RU)}$		X								
22	FIA_AFL.1$_{(CS)}$						X				
23	FIA_AFL.1$_{(RU)}$						X				
24	FIA_ATD.1$_{(SYS)}$			X							
25	FIA_UAU.2$_{(SYS)}$				X		X			X	

Table 6.8 - Necessity of TOE Requirements

		O.DETECT$_{(RU)}$	O.MEDIA$_{(RU)}$	O.ACCESS$_{(SYS)}$	O.AUDIT$_{(SYS)}$	O.BANNER$_{(SYS)}$	O.IDENTIFY$_{(SYS)}$	O.MANAGE$_{(SYS)}$	O.NO_EAVESDROP$_{(SYS)}$	O.RECEIVE$_{(SYS)}$	O.SELF-PROTECT$_{(SYS)}$
26	FIA_UAU.3$_{(SYS)}$						X				
27	FIA_UAU.6$_{(RU)}$		X								
28	FIA_UAU.7$_{(SYS)}$						X				
29	FIA_UID.2$_{(SYS)}$				X		X				
30	FIA_USB.1$_{(CS)}$				X						
31	FMT_MOF.1$_{(SYS)}$					X		X			
32	FMT_MSA.1$_{(SYS)}$							X			
33	FMT_MSA.2$_{(SYS)}$							X	X		
34	FMT_MSA.3$_{(SYS)}$							X			
35	FMT_MTD.1$_{(SYS)}$							X			
36	FMT_REV.1$_{(SYS)}$							X			
37	FMT_SAE.1$_{(CS)}$							X			
38	FMT_SMR.1$_{(SYS)}$							X			
39	FPT_FLS.1$_{(CS)}$										X
40	FPT_FLS.1$_{(RU)}$										X
41	FPT_ITT.2$_{(SYS)}$										X
42	FPT_ITT.3$_{(SYS)}$										X
43	FPT_RPL.1$_{(SYS)}$										X
44	FPT_RVM.1$_{(SYS)}$										X
45	FPT_SEP.1$_{(SYS)}$										X
46	FPT_STM.1$_{(CS)}$				X						
47	FTA_SSL.1$_{(RU)}$		X								
48	FTA_TAB.1$_{(SYS)}$					X					

182

183

6.7.3 NECESSITY ARGUMENT FOR ASSUMPTIONS AND OBJECTIVES

184 The following table maps TOE objectives to policies and threats. Note that P.MARKING, while not covered by TOE objectives, is addressed through assumptions and environmental objectives. (See Table 6.10.)

Table 6.9 - Necessity of TOE Objectives

TOE Objectives	P.ACCOUNT	P.CONFIDENTIALITY	P.ELGIBLE	P.EXPORT	P.INTEGRITY	P.MANAGE	P.MARKING	T.ALTER	T.CAPTURE	T.CRASH	T.ERROR	T.IMPORT	T.INTRUDE	T.MASQUERADE	T.PHYSICAL	T.TRAFFIC
$O.ACCESS_{(SYS)}$		X	X		X								X			
$O.AUDIT_{(SYS)}$	X															
$O.BANNER_{(SYS)}$	X															
$O.DETECT_{(RU)}$					X			X			X	X	X		X	
$O.IDENTIFY_{(SYS)}$	X	X			X								X	X	X	
$O.MANAGE_{(SYS)}$						X										
$O.MEDIA_{(RU)}$		X	X	X							X		X			
$O.NO\_EAVESDROP_{(SYS)}$		X	X	X					X							X
$O.RECEIVE_{(SYS)}$		X		X	X				X		X		X			
$O.SELF\text{-}PROTECT_{(SYS)}$									X	X		X				

6.7.4 NECESSITY ARGUMENT FOR ASSUMPTIONS AND ENVIRONMENTAL OBJECTIVES

185 The following table maps assumptions and environmental objectives to policies, threats, and assumptions (as applicable). Note that T.CRASH and T.MASQUERADE, while not covered by assumptions or environmental objectives, are addressed through TOE objectives. (See Table 6.9.)

Table 6.10 - Necessity of Assumptions and Environmental Objectives

Assumptions and Environmental Objectives	A.CONTROLLED$_{(RU)}$	A.DEDICATED$_{(CS)}$	A.FACILITY$_{(CS)}$	A.TRUSTED_ADMIN$_{(SYS)}$	A.TRUSTED_USER$_{(SYS)}$	P.ACCOUNT	P.CONFIDENTIALITY	P.ELGIBLE	P.EXPORT	P.INTEGRITY	P.MANAGE	P.MARKING	T.ALTER	T.CAPTURE	T.CRASH	T.ERROR	T.IMPORT	T.INTRUDE	T.MASQUERADE	T.PHYSICAL	T.TRAFFIC
A.CONTROLLED$_{(RU)}$	N/A										X										
A.DEDICATED$_{(CS)}$						X											X			X	
A.FACILITY$_{(CS)}$						X	X		X	X		X	X							X	
A.TRUSTED_ADMIN$_{(SYS)}$						X	X	X	X	X	X	X	X			X					
A.TRUSTED_USER$_{(SYS)}$							X	X	X	X		X	X			X					
OE.ACCREDITED$_{(SYS)}$			X						X												
OE.ADMIN$_{(SYS)}$	X	X																			
OE.AUDIT$_{(CS)}$						X															
OE.CLEARED$_{(SYS)}$				X	X							X								X	
OE.CRYPTOKEYS$_{(SYS)}$							X	X	X	X				X		X					
OE.INSTALL$_{(SYS)}$	X	X									X						X				
OE.OPERATE$_{(RU)}$	X												X	X			X	X		X	X
OE.PHYSICAL$_{(SYS)}$	X		X					X					X	X				X		X	
OE.TRAINED$_{(SYS)}$				X	X						X	X					X				

REFERENCES

[1] Common Criteria Implementation Board. Common Criteria for Information Technology Security Evaluation, Version 2.1. CCIMB-99-021, 032, 033. August 1999.

[2] Common Criteria for Information Technology Security Evaluation, Version 1.0. August, 1999.

[3] ISO/IEC JTC 1/SC 27/WG 3. Guide for Production of PPs and STs, N452, Version .6 (draft), July 1998.

[4] Executive Order 12958, "Classified National Security Information," April 17, 1995. The White House: Office of the Press Secretary. Washington, DC.

[5] DoD Directive 85xx.M&L (DRAFT), "Electronic Marking and Labeling," September 25, 1998. The Department of Defense, ASD(C3I): Washington, DC.

[6] OMB Circular No. A-130, "Management of Federal Information Resources," February 8, 1996. Office of Management and Budget: Washington, DC.

[7] Memorandum from ASD(C3I), subject “Policy on Department of Defense (DoD) Electronic Notice and Consent Banner,” 16 January 1997. The Department of Defense, ASD(C3I): Washington, DC.

[8] U.S. DoD Remote Access Protection Profile for SBU-High Environments. Department of Defense: October 7, 1999.

[9] U.S. DoD Communications Server Protection Profile. Department of Defense:

ACRONYMS

The following abbreviations from the Common Criteria are used in this Protection Profile:

BIOS	Basic Input/Output System
CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
RAM	Random Access Memory
SFP	Security Function Policy
SoF	Strength-of-Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy